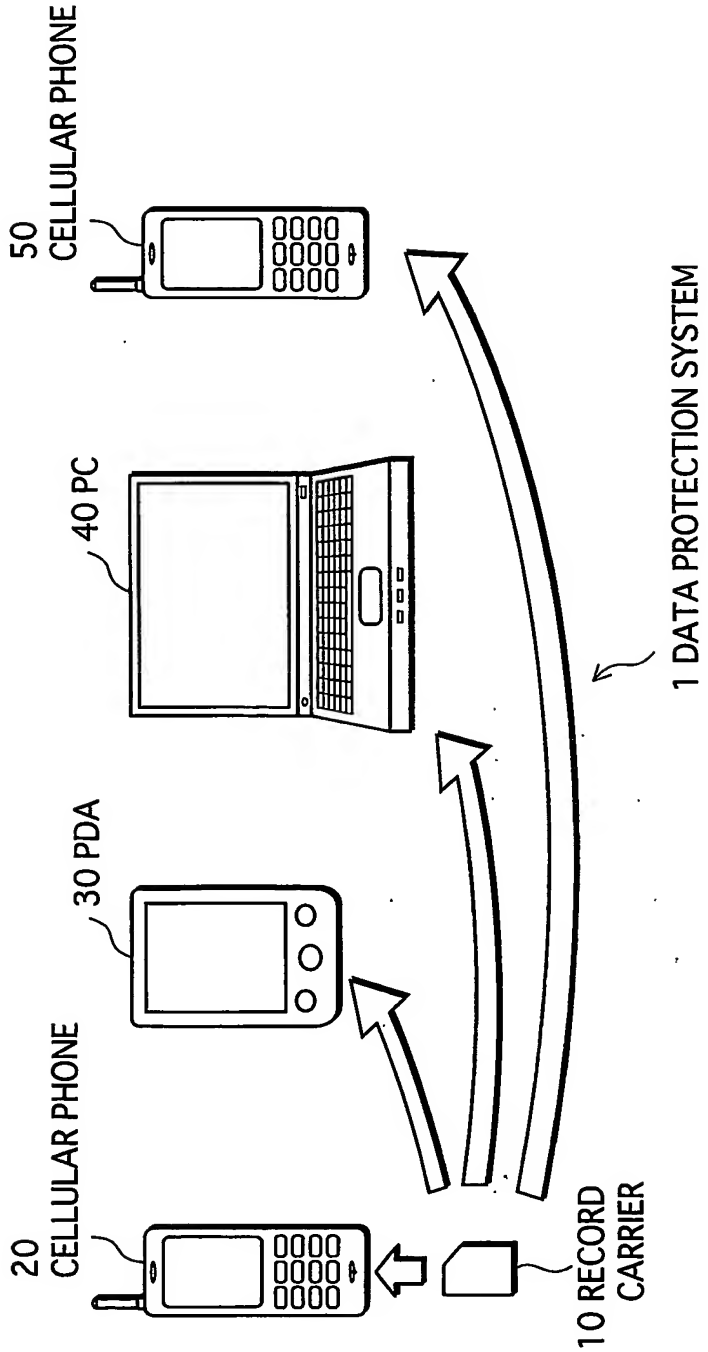

50
CELLULAR PHONE
40 PC
30 PDA
20
CELLULAR PHONE
10 RECORD
CARRIER
1 DATA PROTECTION SYSTEM

FIG.1

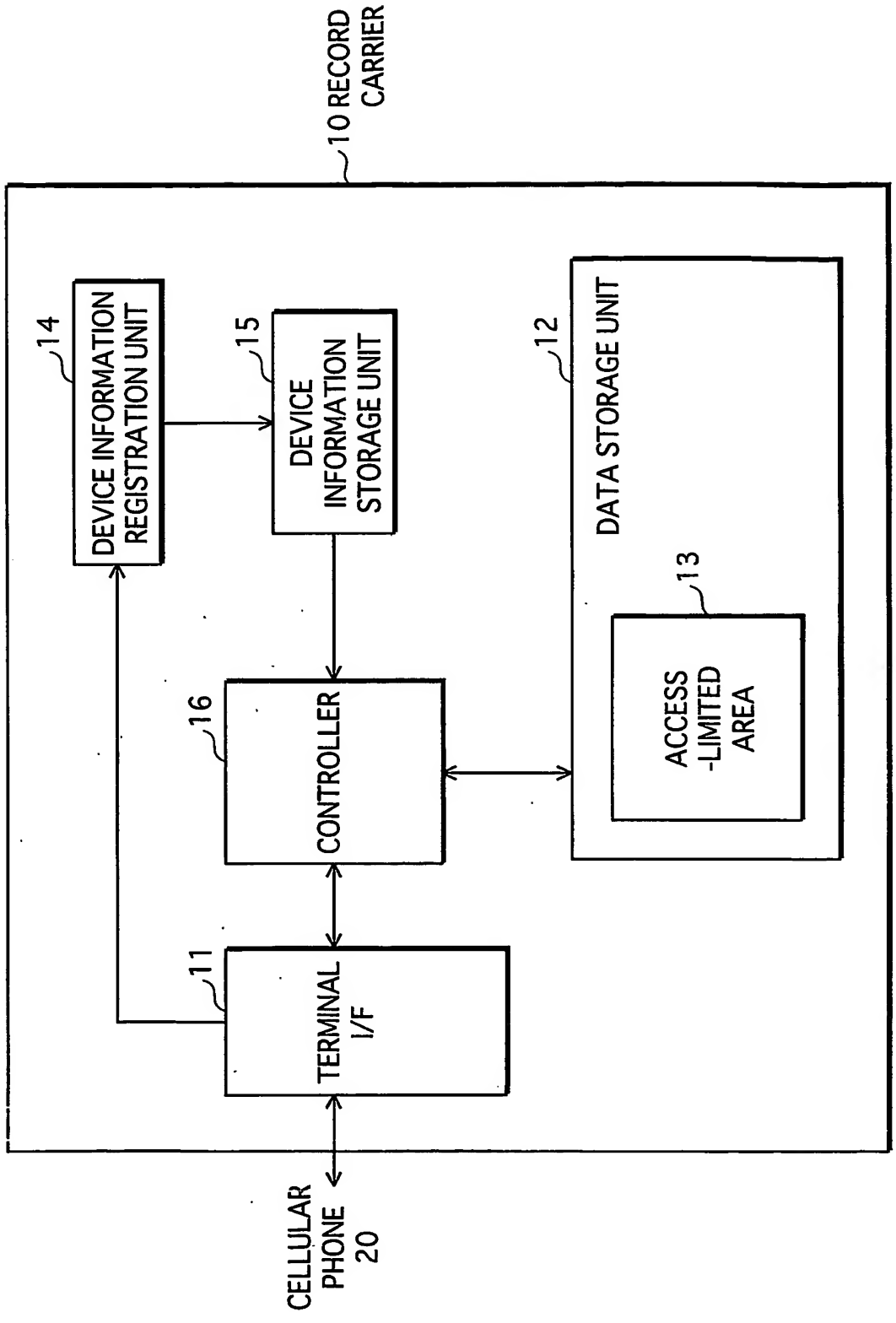

10 RECORD CARRIER
14
DEVICE INFORMATION REGISTRATION UNIT
15
DEVICE INFORMATION STORAGE UNIT
12
DATA STORAGE UNIT
13
ACCESS -LIMITED AREA
16
CONTROLLER
11
TERMINAL I/F
CELLULAR PHONE 20

FIG.2

FIG.3

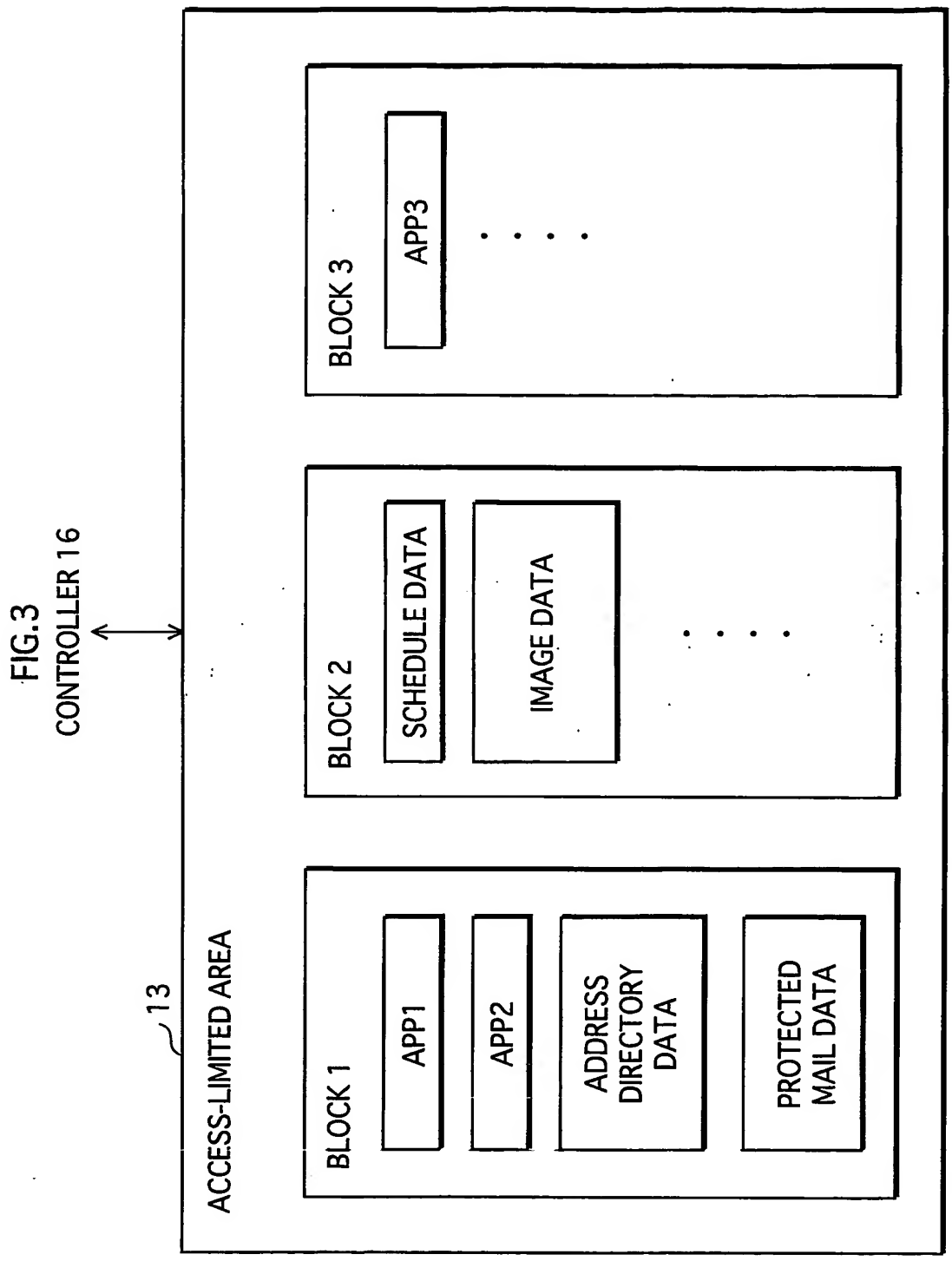

CONTROLLER 16
13
ACCESS-LIMITED AREA
BLOCK 1
APP1
APP2
ADDRESS DIRECTORY DATA
PROTECTED MAIL DATA
BLOCK 2
SCHEDULE DATA
IMAGE DATA
BLOCK 3
APP3

FIG.4

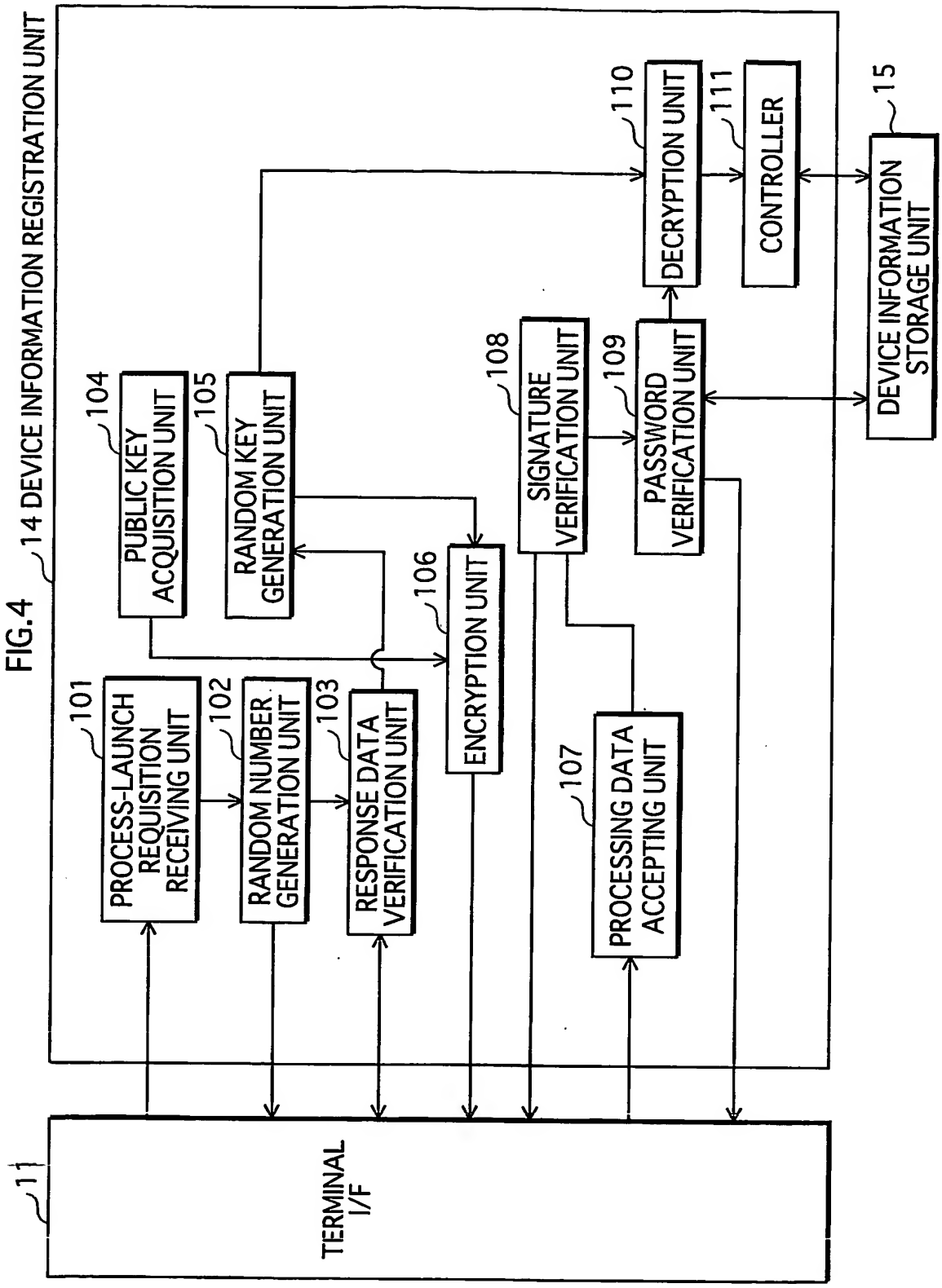

14 DEVICE INFORMATION REGISTRATION UNIT
PROCESS-LAUNCH REQUISITION RECEIVING UNIT
101
RANDOM NUMBER GENERATION UNIT
102
RESPONSE DATA VERIFICATION UNIT
103
PUBLIC KEY ACQUISITION UNIT
104
RANDOM KEY GENERATION UNIT
105
ENCRYPTION UNIT
106
PROCESSING DATA ACCEPTING UNIT
107
SIGNATURE VERIFICATION UNIT
108
PASSWORD VERIFICATION UNIT
109
DECRYPTION UNIT
110
CONTROLLER
111
DEVICE INFORMATION STORAGE UNIT
15
TERMINAL I/F
11

FIG.5

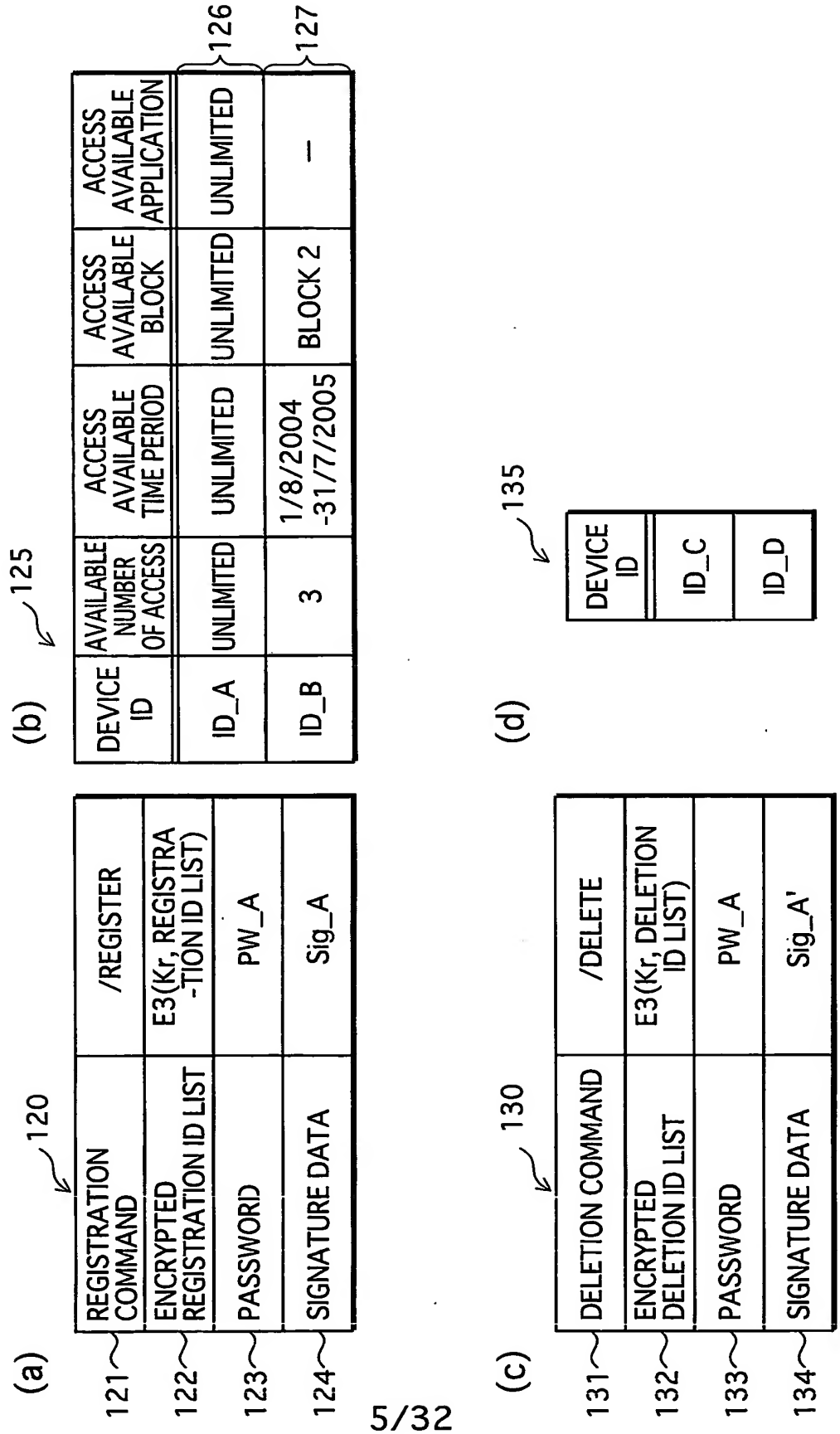

(a)
120
REGISTRATION COMMAND
/REGISTER
ENCRYPTED REGISTRATION ID LIST
E3(Kr, REGISTRA-TION ID LIST)
PASSWORD
PW_A
SIGNATURE DATA
Sig_A
121
122
123
124
(b)
125
DEVICE ID
AVAILABLE NUMBER OF ACCESS
ACCESS AVAILABLE TIME PERIOD
ACCESS AVAILABLE BLOCK
ACCESS AVAILABLE APPLICATION
ID_A
UNLIMITED
UNLIMITED
UNLIMITED
UNLIMITED
ID_B
3
1/8/2004 -31/7/2005
BLOCK 2
—
126
127
(c)
130
DELETION COMMAND
/DELETE
ENCRYPTED DELETION ID LIST
E3(Kr, DELETION ID LIST)
PASSWORD
PW_A
SIGNATURE DATA
Sig_A'
131
132
133
134
(d)
135
DEVICE ID
ID_C
ID_D

FIG.6

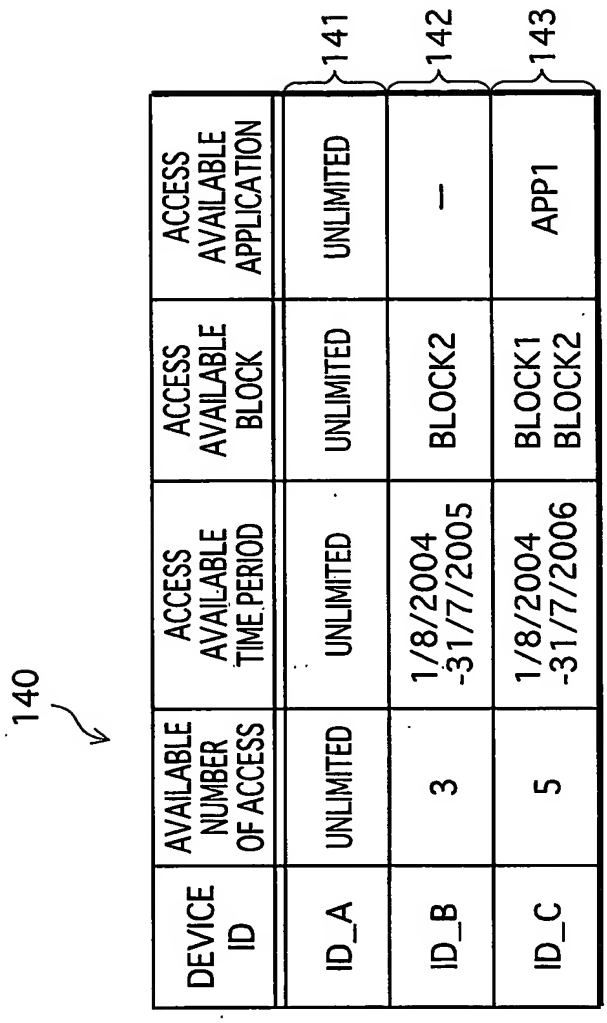

140
141
142
143
DEVICE ID
AVAILABLE NUMBER OF ACCESS
ACCESS AVAILABLE TIME PERIOD
ACCESS AVAILABLE BLOCK
ACCESS AVAILABLE APPLICATION
ID_A
UNLIMITED
UNLIMITED
UNLIMITED
UNLIMITED
ID_B
3
1/8/2004 -31/7/2005
BLOCK2
—
ID_C
5
1/8/2004 -31/7/2006
BLOCK1 BLOCK2
APP1

FIG.7

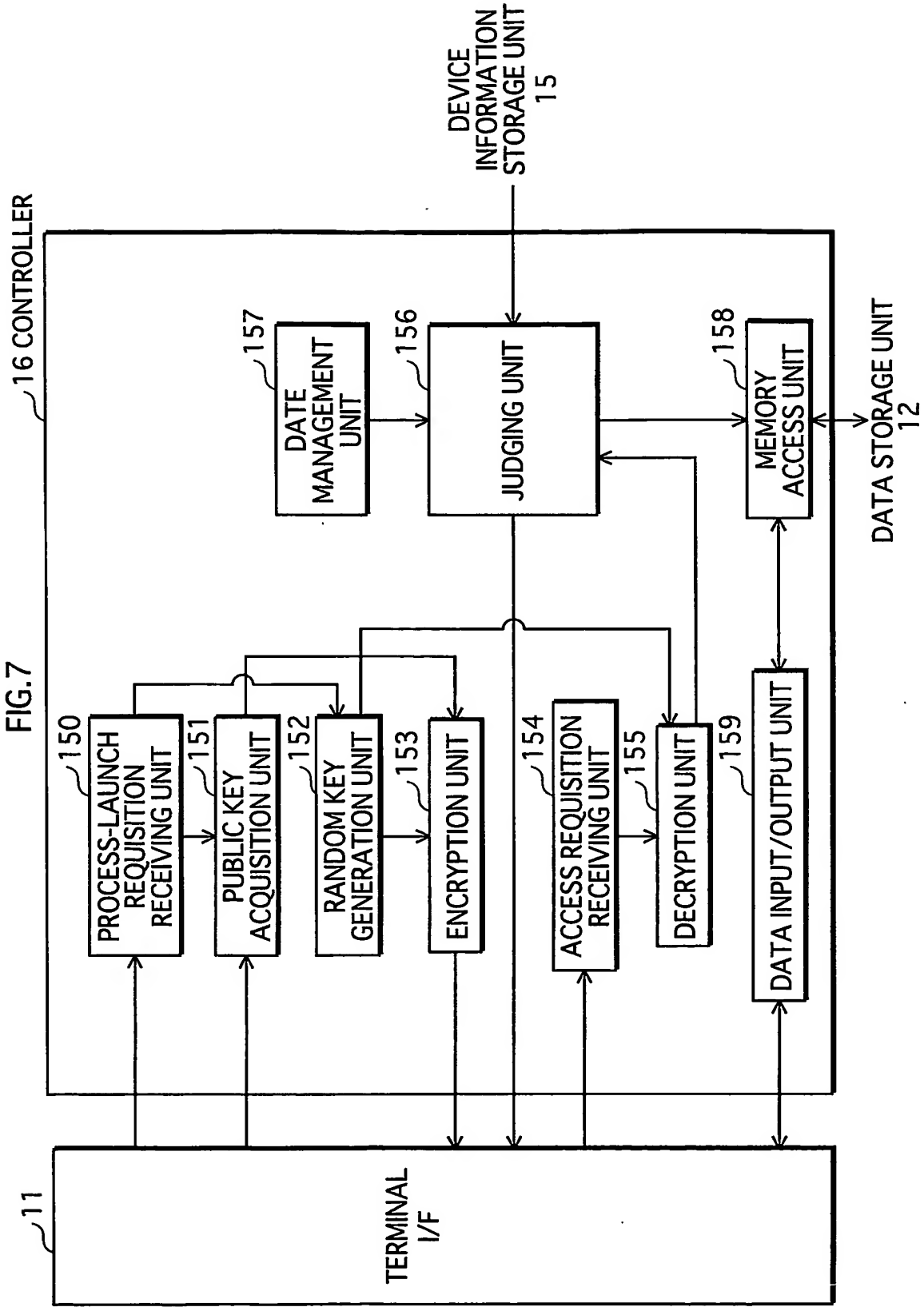

DEVICE INFORMATION STORAGE UNIT 15
16 CONTROLLER
157 DATE MANAGEMENT UNIT
156 JUDGING UNIT
158 MEMORY ACCESS UNIT
DATA STORAGE UNIT 12
150 PROCESS-LAUNCH REQUISITION RECEIVING UNIT
151 PUBLIC KEY ACQUISITION UNIT
152 RANDOM KEY GENERATION UNIT
153 ENCRYPTION UNIT
154 ACCESS REQUISITION RECEIVING UNIT
155 DECRYPTION UNIT
159 DATA INPUT/OUTPUT UNIT
11 TERMINAL I/F

FIG.8

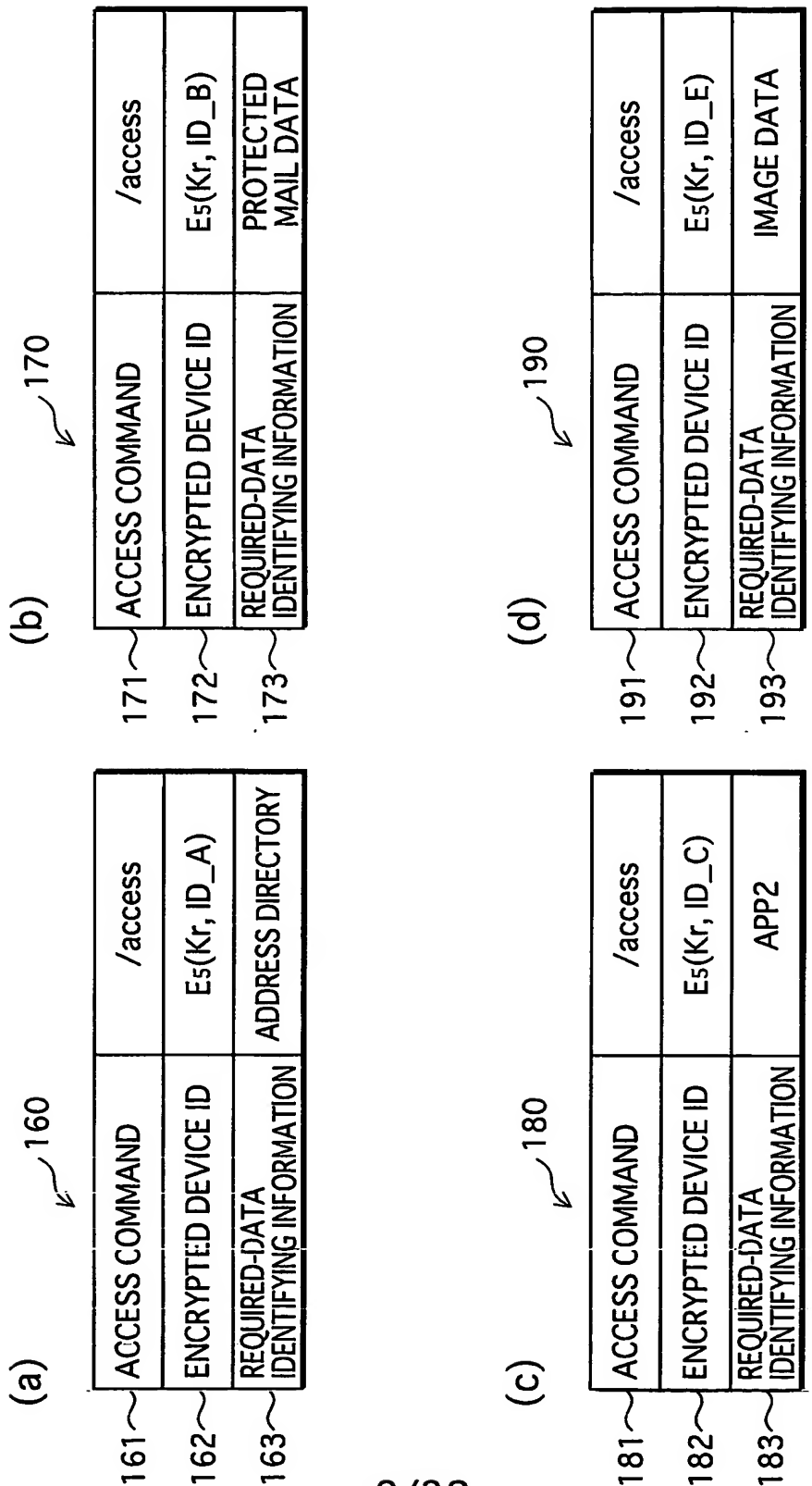

(a)
160
161
ACCESS COMMAND
/access
162
ENCRYPTED DEVICE ID
E5(Kr, ID_A)
163
REQUIRED-DATA IDENTIFYING INFORMATION
ADDRESS DIRECTORY
(b)
170
171
ACCESS COMMAND
/access
172
ENCRYPTED DEVICE ID
E5(Kr, ID_B)
173
REQUIRED-DATA IDENTIFYING INFORMATION
PROTECTED MAIL DATA
(c)
180
181
ACCESS COMMAND
/access
182
ENCRYPTED DEVICE ID
E5(Kr, ID_C)
183
REQUIRED-DATA IDENTIFYING INFORMATION
APP2
(d)
190
191
ACCESS COMMAND
/access
192
ENCRYPTED DEVICE ID
E5(Kr, ID_E)
193
REQUIRED-DATA IDENTIFYING INFORMATION
IMAGE DATA

FIG.9

200

BLOCK NUMBER	DATA IDENTIFYING INFORMATION
1	APP1 APP2 ADDRESS DIRECTORY DATA PROTECTED MAIL DATA
2	SCHEDULE DATA IMAGE DATA • • •
3	APP3 • • •

FIG.10

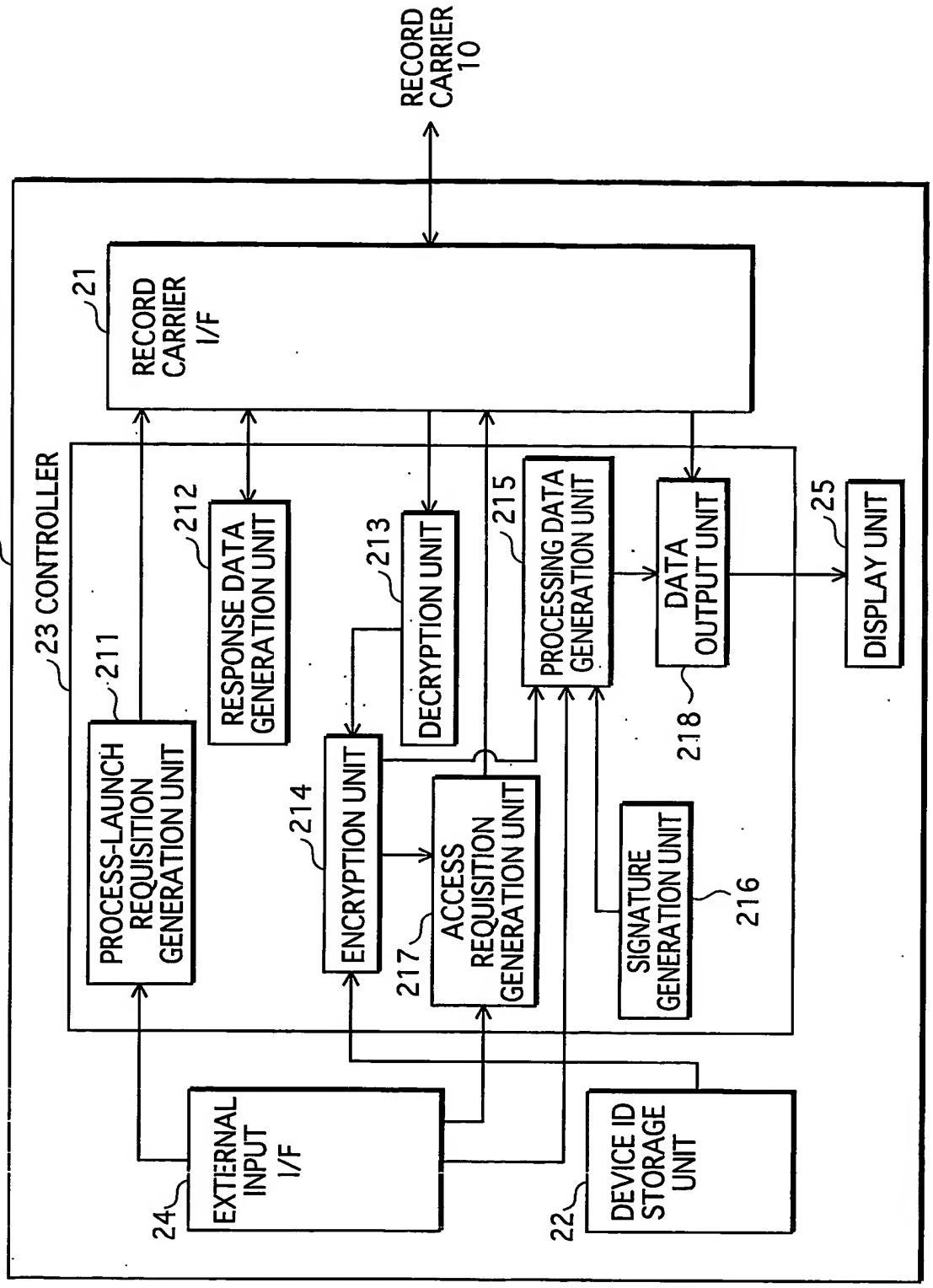

RECORD CARRIER 10
20 CELLULAR PHONE
21
RECORD CARRIER I/F
23 CONTROLLER
211
PROCESS-LAUNCH REQUISITION GENERATION UNIT
212
RESPONSE DATA GENERATION UNIT
213
DECRYPTION UNIT
214
ENCRYPTION UNIT
215
PROCESSING DATA GENERATION UNIT
216
SIGNATURE GENERATION UNIT
217
ACCESS REQUISITION GENERATION UNIT
218
DATA OUTPUT UNIT
25
DISPLAY UNIT
24
EXTERNAL INPUT I/F
22
DEVICE ID STORAGE UNIT

FIG.11

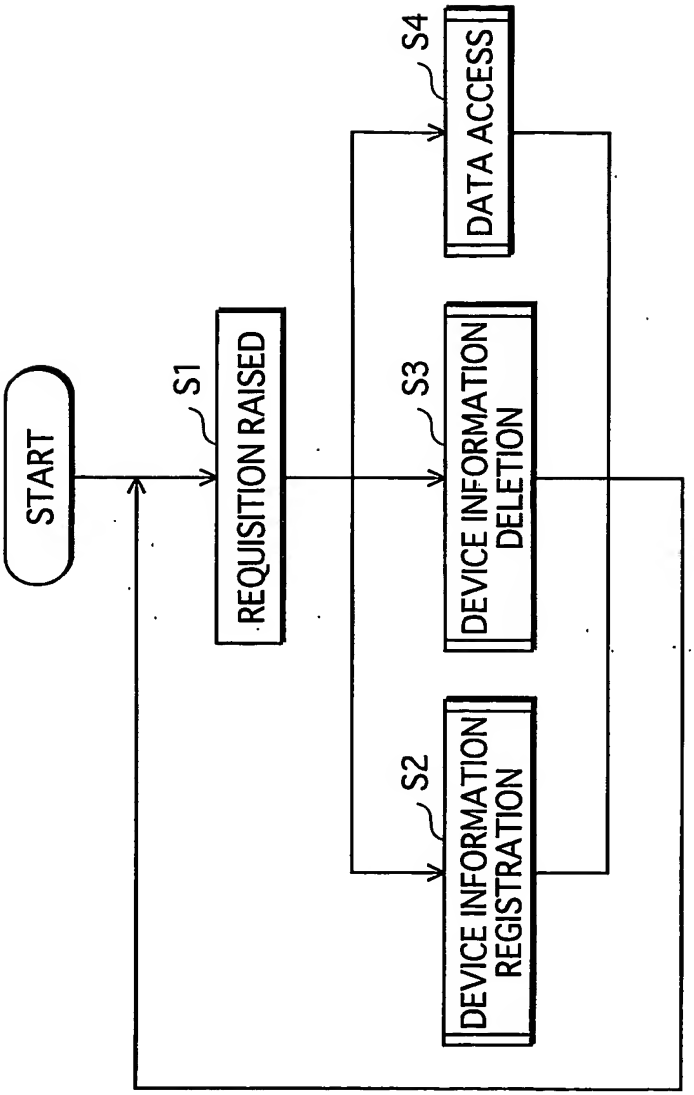

START
S1
REQUISITION RAISED
S2
DEVICE INFORMATION REGISTRATION
S3
DEVICE INFORMATION DELETION
S4
DATA ACCESS

FIG.12

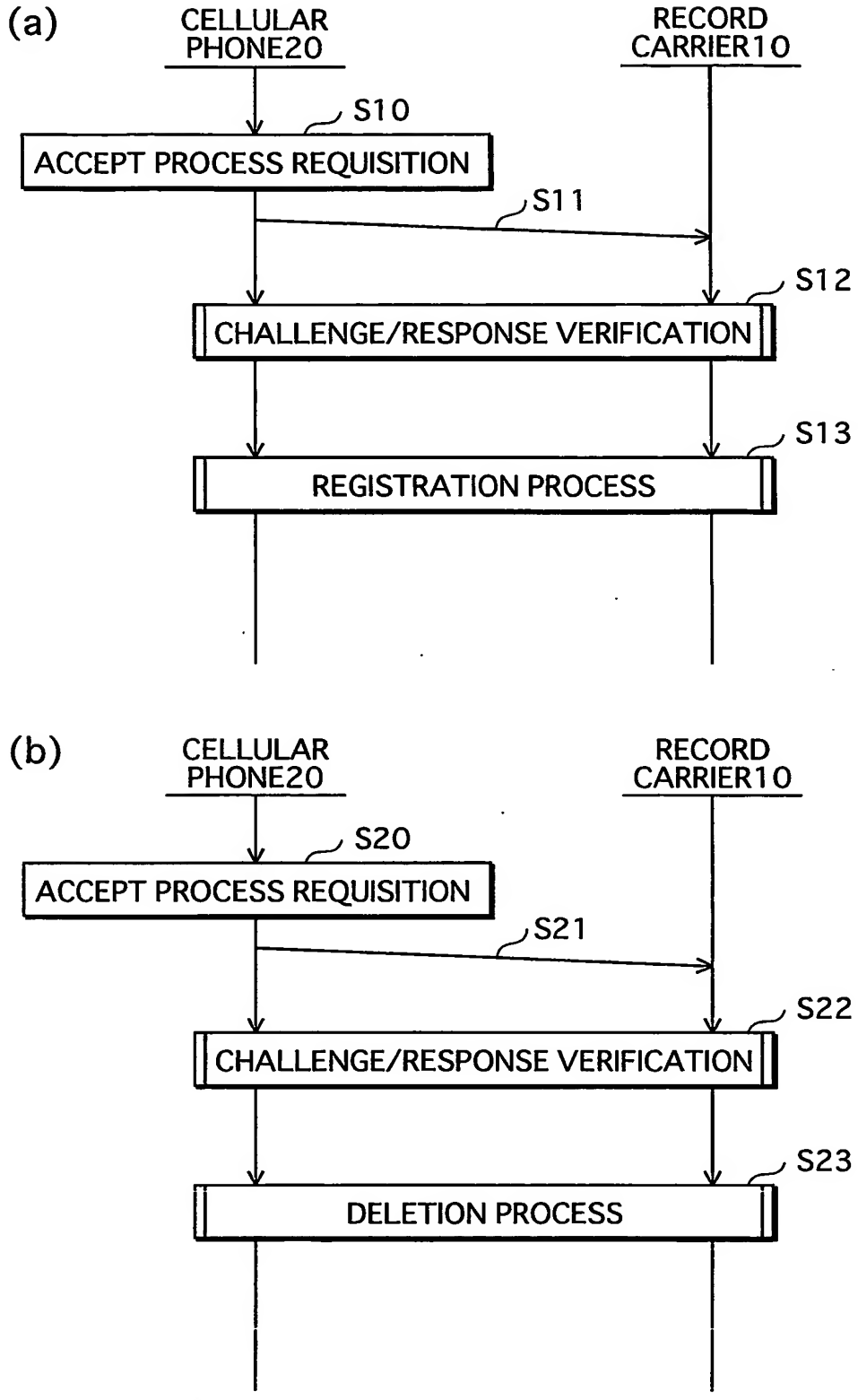

(a)
CELLULAR PHONE20
RECORD CARRIER10
S10
ACCEPT PROCESS REQUISITION
S11
S12
CHALLENGE/RESPONSE VERIFICATION
S13
REGISTRATION PROCESS
(b)
CELLULAR PHONE20
RECORD CARRIER10
S20
ACCEPT PROCESS REQUISITION
S21
S22
CHALLENGE/RESPONSE VERIFICATION
S23
DELETION PROCESS

FIG.13

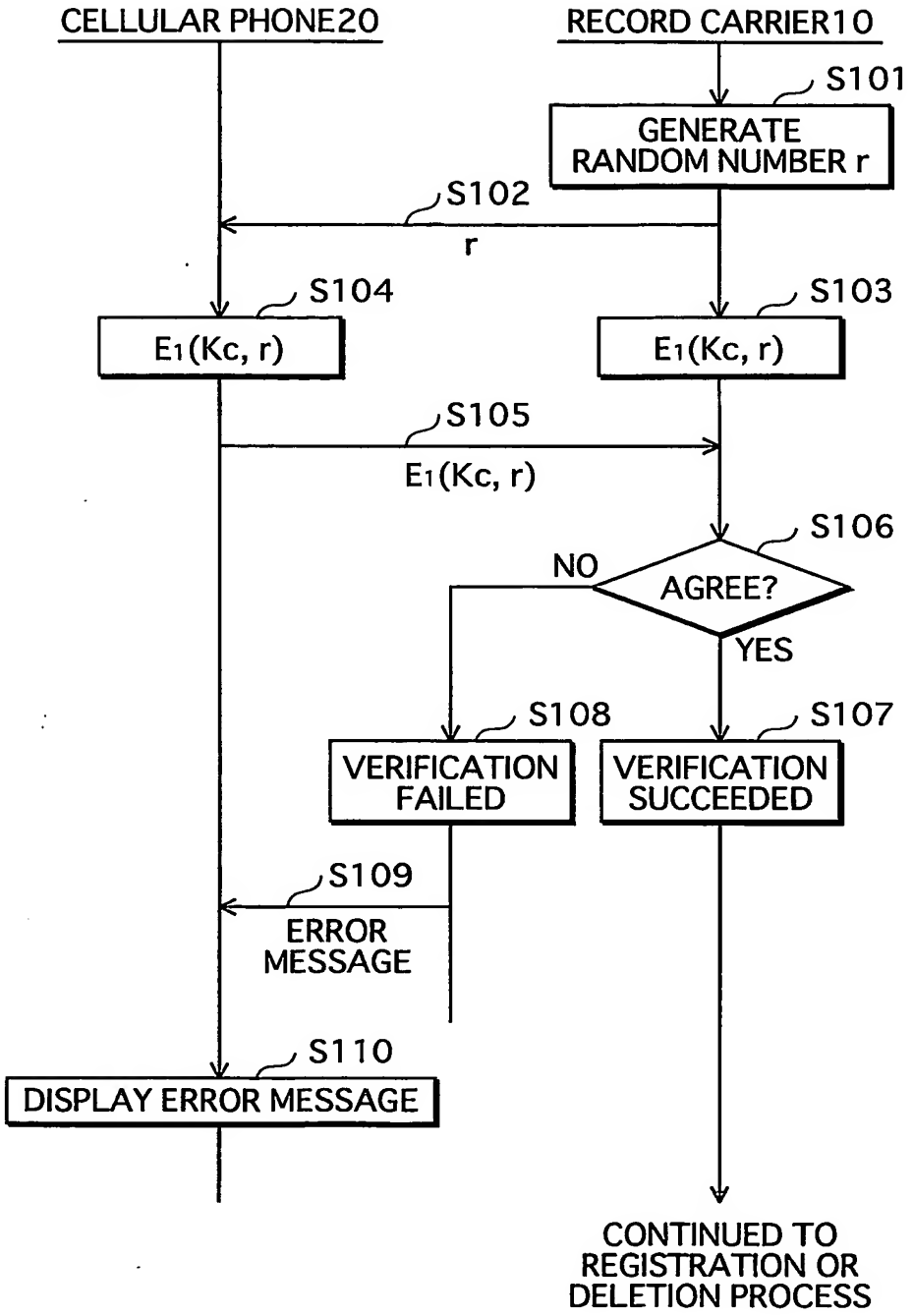

CELLULAR PHONE20
RECORD CARRIER10
S101
GENERATE RANDOM NUMBER r
S102
r
S104
E1(Kc, r)
S103
E1(Kc, r)
S105
E1(Kc, r)
S106
NO
AGREE?
YES
S108
VERIFICATION FAILED
S107
VERIFICATION SUCCEEDED
S109
ERROR MESSAGE
S110
DISPLAY ERROR MESSAGE
CONTINUED TO REGISTRATION OR DELETION PROCESS

FIG.14

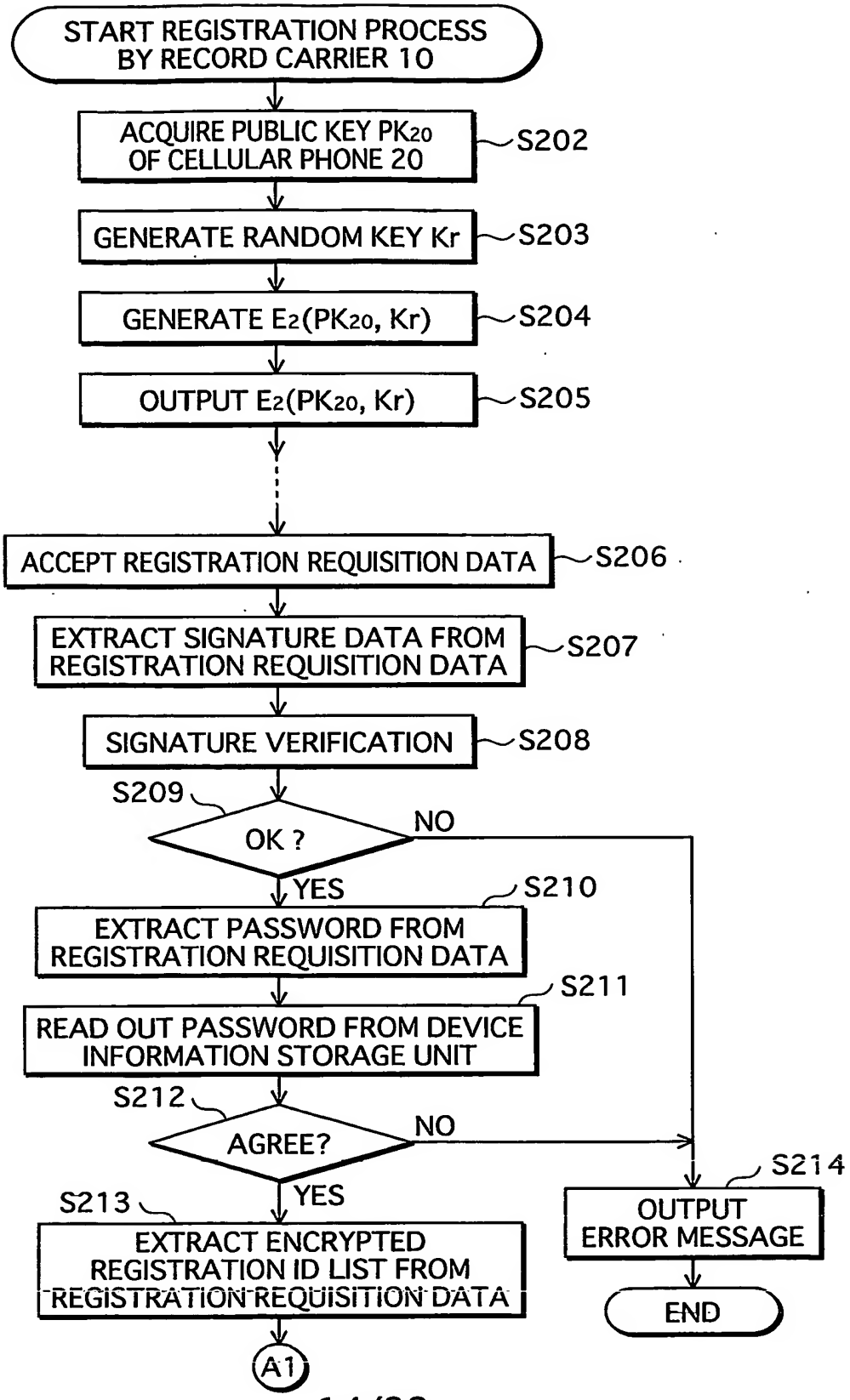

START REGISTRATION PROCESS BY RECORD CARRIER 10
ACQUIRE PUBLIC KEY PK20 OF CELLULAR PHONE 20
S202
GENERATE RANDOM KEY Kr
S203
GENERATE E2(PK20, Kr)
S204
OUTPUT E2(PK20, Kr)
S205
ACCEPT REGISTRATION REQUISITION DATA
S206
EXTRACT SIGNATURE DATA FROM REGISTRATION REQUISITION DATA
S207
SIGNATURE VERIFICATION
S208
S209
OK ?
NO
YES
S210
EXTRACT PASSWORD FROM REGISTRATION REQUISITION DATA
S211
READ OUT PASSWORD FROM DEVICE INFORMATION STORAGE UNIT
S212
AGREE?
NO
YES
S213
EXTRACT ENCRYPTED REGISTRATION ID LIST FROM REGISTRATION REQUISITION DATA
A1
S214
OUTPUT ERROR MESSAGE
END

FIG.15

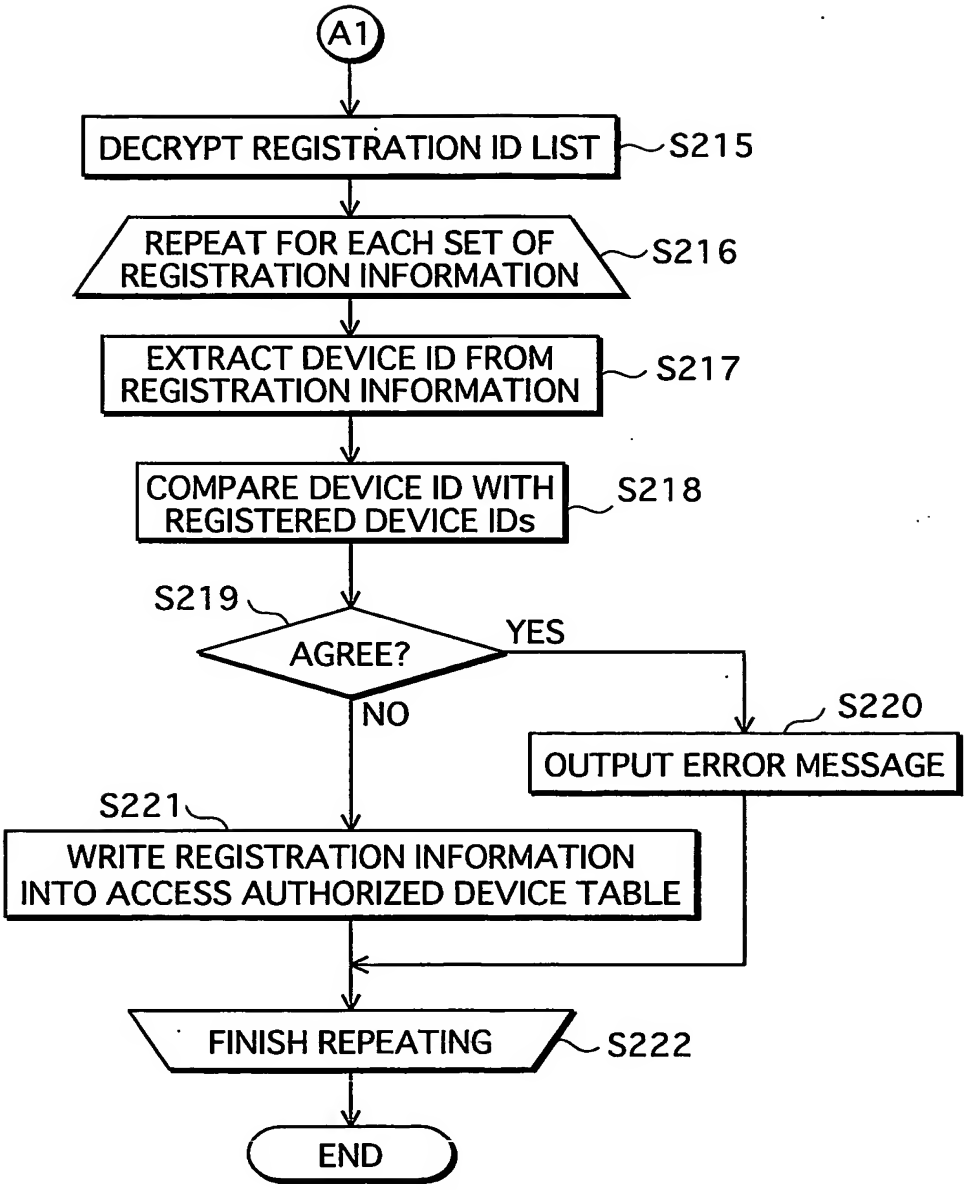

A1
DECRYPT REGISTRATION ID LIST
S215
REPEAT FOR EACH SET OF REGISTRATION INFORMATION
S216
EXTRACT DEVICE ID FROM REGISTRATION INFORMATION
S217
COMPARE DEVICE ID WITH REGISTERED DEVICE IDs
S218
S219
AGREE?
YES
NO
S220
OUTPUT ERROR MESSAGE
S221
WRITE REGISTRATION INFORMATION INTO ACCESS AUTHORIZED DEVICE TABLE
FINISH REPEATING
S222
END

FIG.16

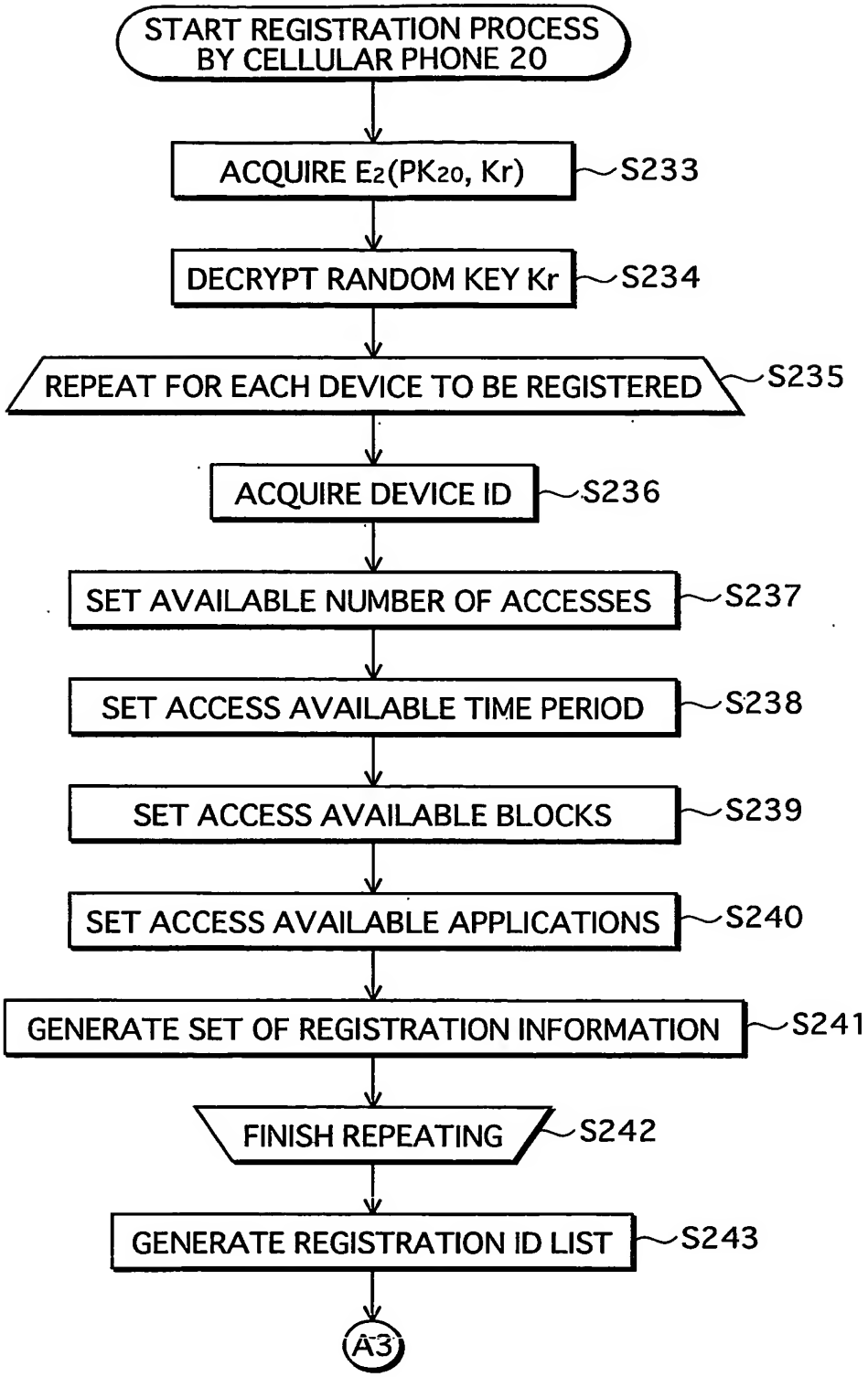

START REGISTRATION PROCESS BY CELLULAR PHONE 20
ACQUIRE E2(PK20, Kr)
S233
DECRYPT RANDOM KEY Kr
S234
REPEAT FOR EACH DEVICE TO BE REGISTERED
S235
ACQUIRE DEVICE ID
S236
SET AVAILABLE NUMBER OF ACCESSES
S237
SET ACCESS AVAILABLE TIME PERIOD
S238
SET ACCESS AVAILABLE BLOCKS
S239
SET ACCESS AVAILABLE APPLICATIONS
S240
GENERATE SET OF REGISTRATION INFORMATION
S241
FINISH REPEATING
S242
GENERATE REGISTRATION ID LIST
S243
A3

FIG.17

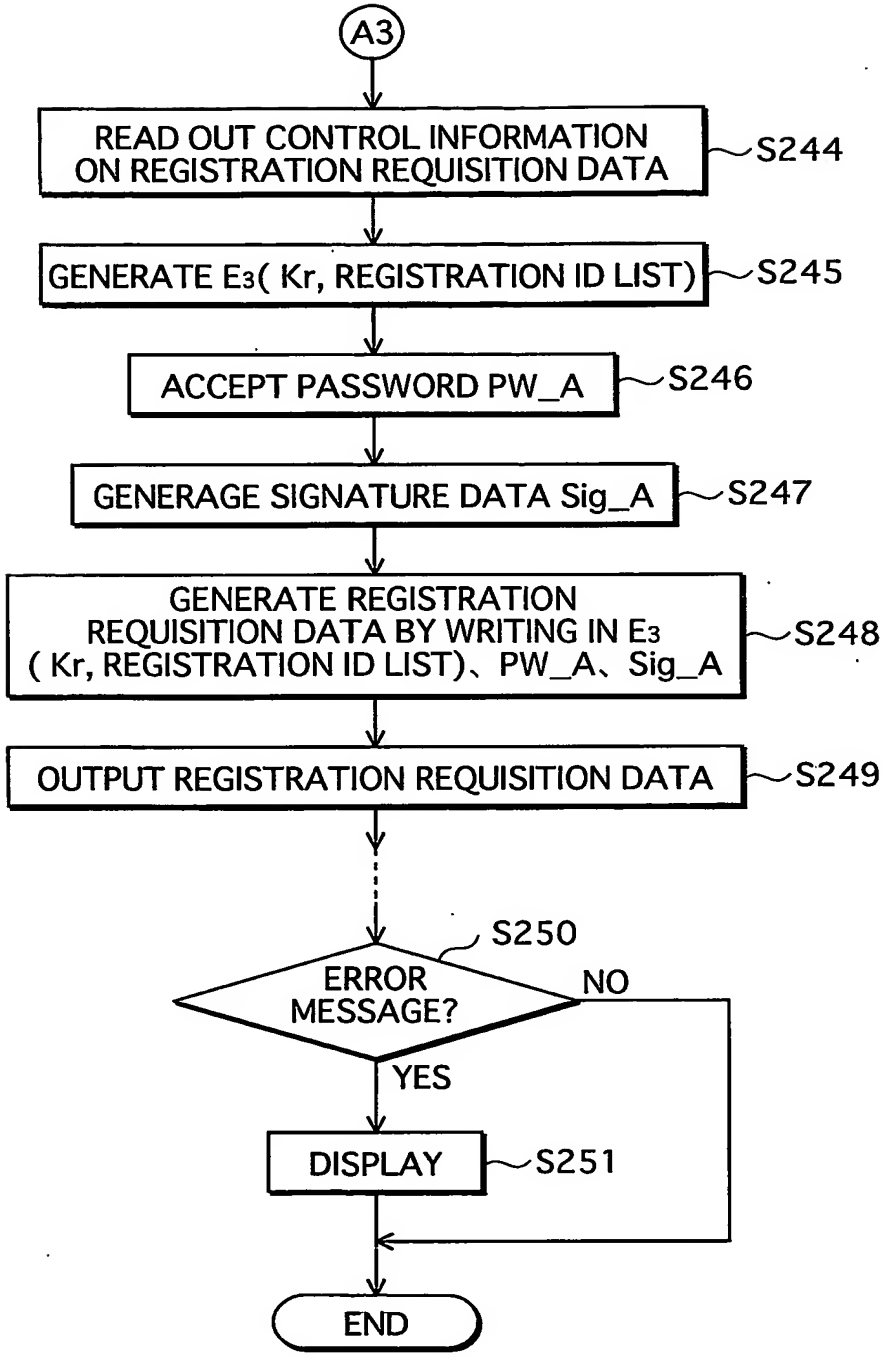

A3
READ OUT CONTROL INFORMATION ON REGISTRATION REQUISITION DATA
S244
GENERATE E3(Kr, REGISTRATION ID LIST)
S245
ACCEPT PASSWORD PW_A
S246
GENERAGE SIGNATURE DATA Sig_A
S247
GENERATE REGISTRATION REQUISITION DATA BY WRITING IN E3 (Kr, REGISTRATION ID LIST)、PW_A、Sig_A
S248
OUTPUT REGISTRATION REQUISITION DATA
S249
S250
ERROR MESSAGE?
NO
YES
DISPLAY
S251
END

FIG.18

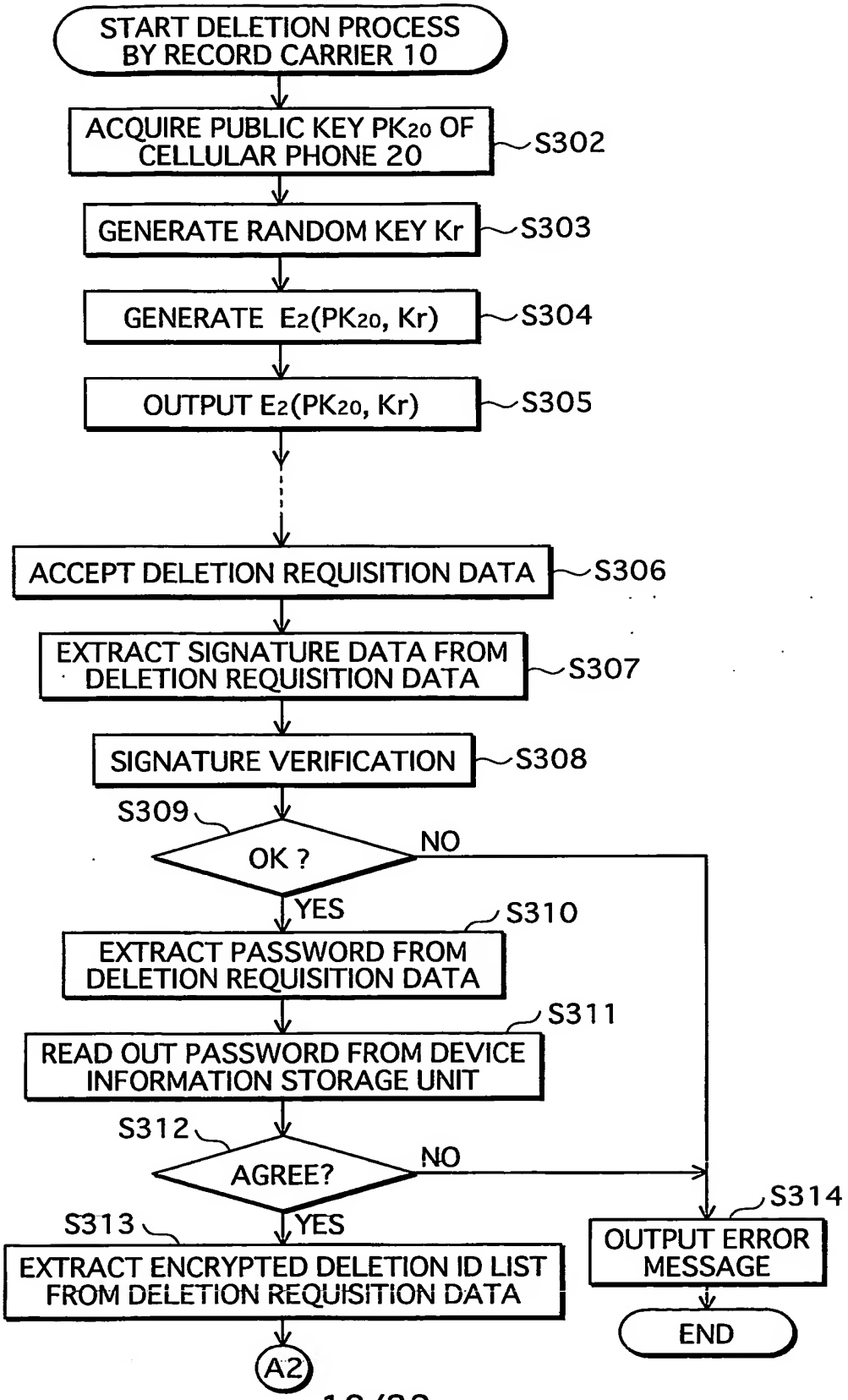

START DELETION PROCESS BY RECORD CARRIER 10
ACQUIRE PUBLIC KEY PK20 OF CELLULAR PHONE 20
S302
GENERATE RANDOM KEY Kr
S303
GENERATE E2(PK20, Kr)
S304
OUTPUT E2(PK20, Kr)
S305
ACCEPT DELETION REQUISITION DATA
S306
EXTRACT SIGNATURE DATA FROM DELETION REQUISITION DATA
S307
SIGNATURE VERIFICATION
S308
S309
OK ?
NO
YES
S310
EXTRACT PASSWORD FROM DELETION REQUISITION DATA
S311
READ OUT PASSWORD FROM DEVICE INFORMATION STORAGE UNIT
S312
AGREE?
NO
YES
S313
EXTRACT ENCRYPTED DELETION ID LIST FROM DELETION REQUISITION DATA
A2
S314
OUTPUT ERROR MESSAGE
END

FIG.19

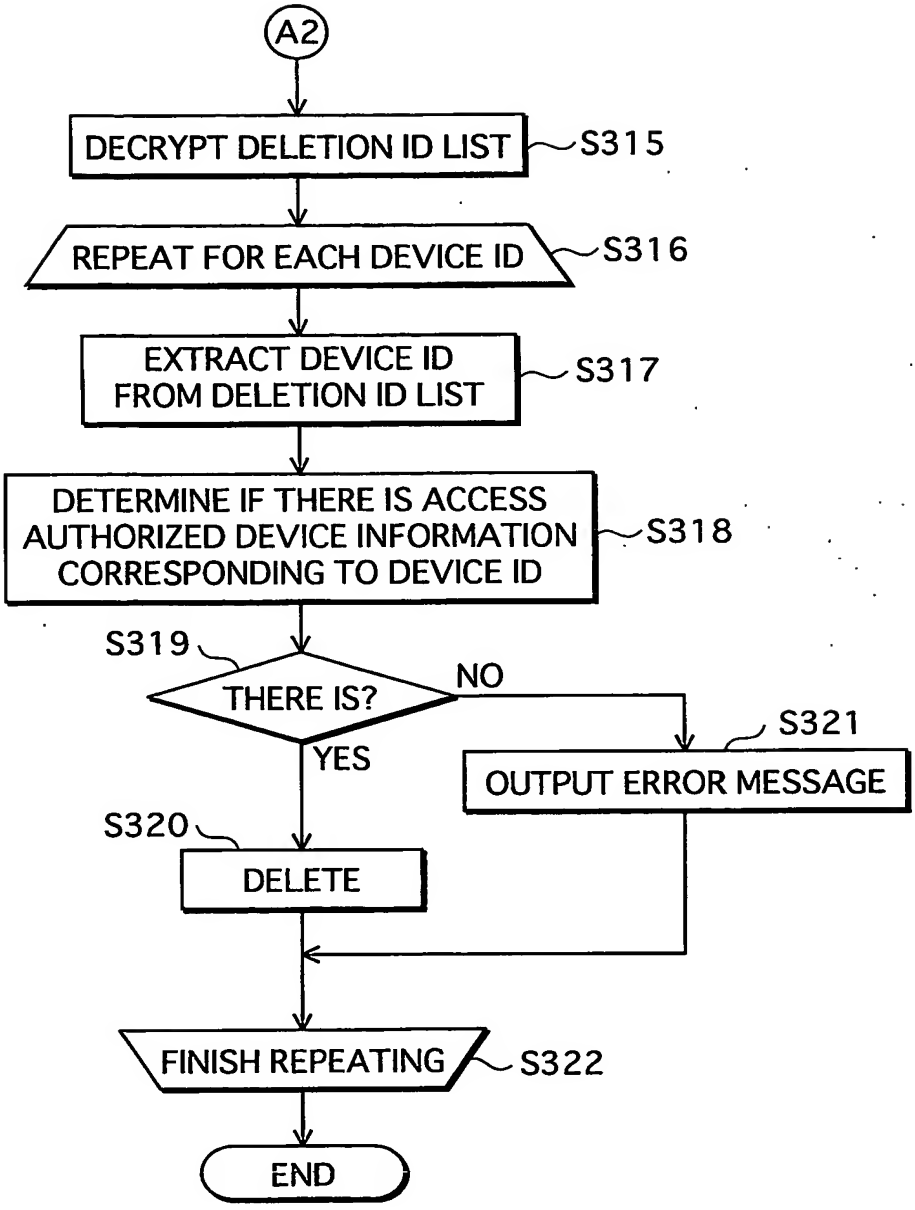

A2
DECRYPT DELETION ID LIST
S315
REPEAT FOR EACH DEVICE ID
S316
EXTRACT DEVICE ID FROM DELETION ID LIST
S317
DETERMINE IF THERE IS ACCESS AUTHORIZED DEVICE INFORMATION CORRESPONDING TO DEVICE ID
S318
S319
THERE IS?
NO
YES
S321
OUTPUT ERROR MESSAGE
S320
DELETE
FINISH REPEATING
S322
END

FIG.20

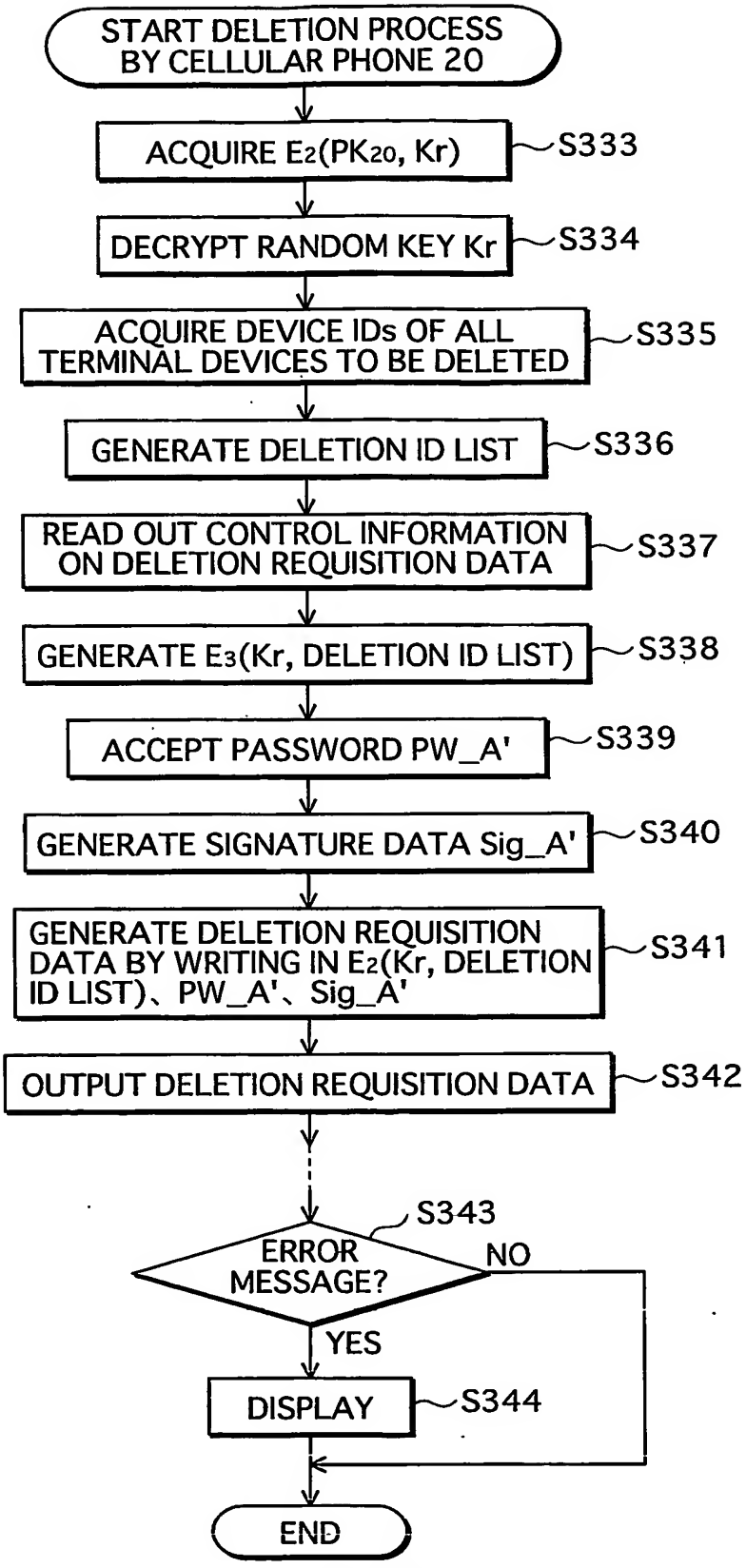

START DELETION PROCESS BY CELLULAR PHONE 20
ACQUIRE E2(PK20, Kr)
S333
DECRYPT RANDOM KEY Kr
S334
ACQUIRE DEVICE IDs OF ALL TERMINAL DEVICES TO BE DELETED
S335
GENERATE DELETION ID LIST
S336
READ OUT CONTROL INFORMATION ON DELETION REQUISITION DATA
S337
GENERATE E3(Kr, DELETION ID LIST)
S338
ACCEPT PASSWORD PW_A'
S339
GENERATE SIGNATURE DATA Sig_A'
S340
GENERATE DELETION REQUISITION DATA BY WRITING IN E2(Kr, DELETION ID LIST)、PW_A'、Sig_A'
S341
OUTPUT DELETION REQUISITION DATA
S342
S343
ERROR MESSAGE?
NO
YES
DISPLAY
S344
END

FIG.21

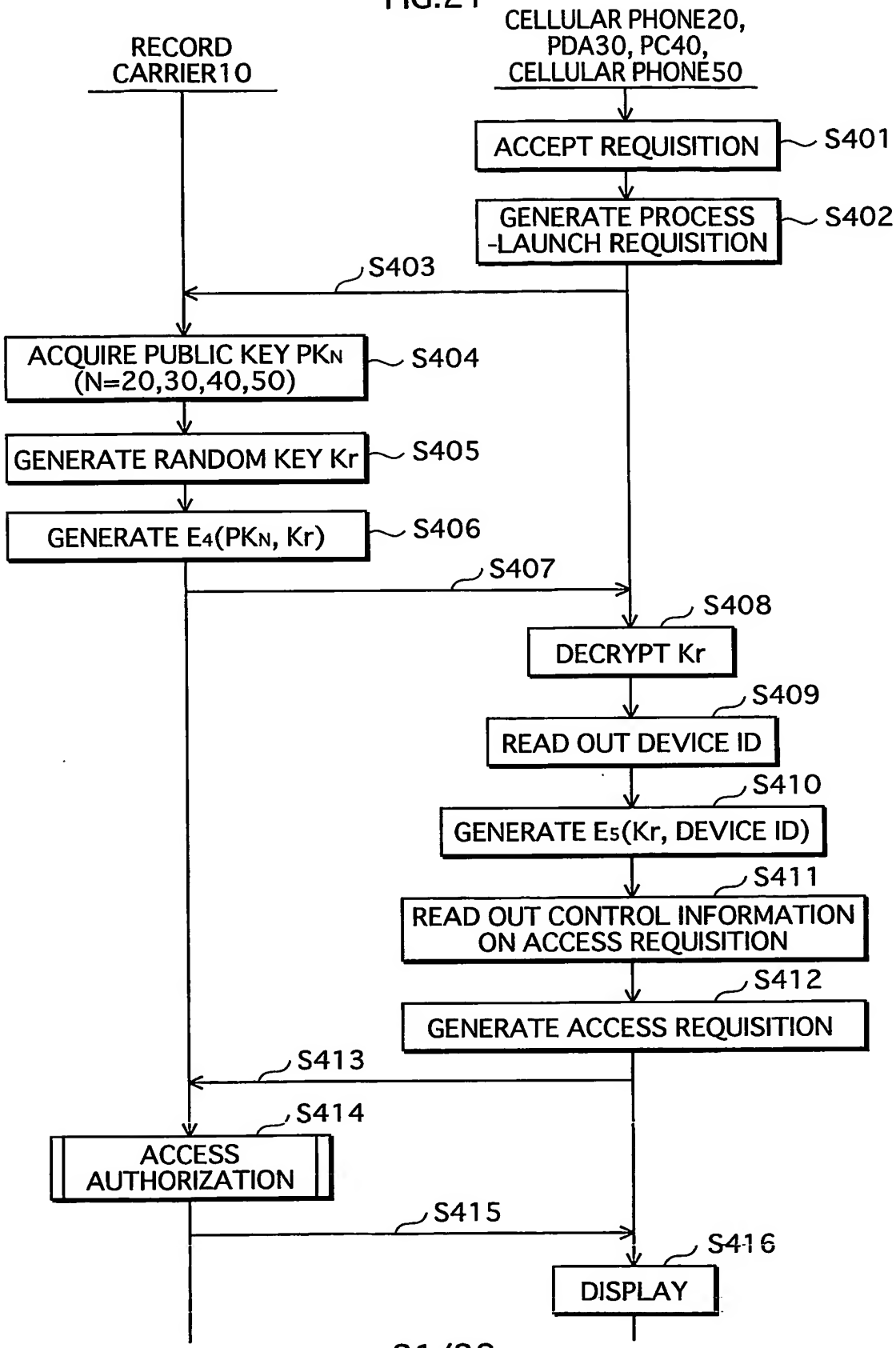

RECORD CARRIER10
CELLULAR PHONE20, PDA30, PC40, CELLULAR PHONE50
ACCEPT REQUISITION
S401
GENERATE PROCESS -LAUNCH REQUISITION
S402
S403
ACQUIRE PUBLIC KEY PKN (N=20,30,40,50)
S404
GENERATE RANDOM KEY Kr
S405
GENERATE E4(PKN, Kr)
S406
S407
S408
DECRYPT Kr
S409
READ OUT DEVICE ID
S410
GENERATE E5(Kr, DEVICE ID)
S411
READ OUT CONTROL INFORMATION ON ACCESS REQUISITION
S412
GENERATE ACCESS REQUISITION
S413
S414
ACCESS AUTHORIZATION
S415
S416
DISPLAY

FIG.22

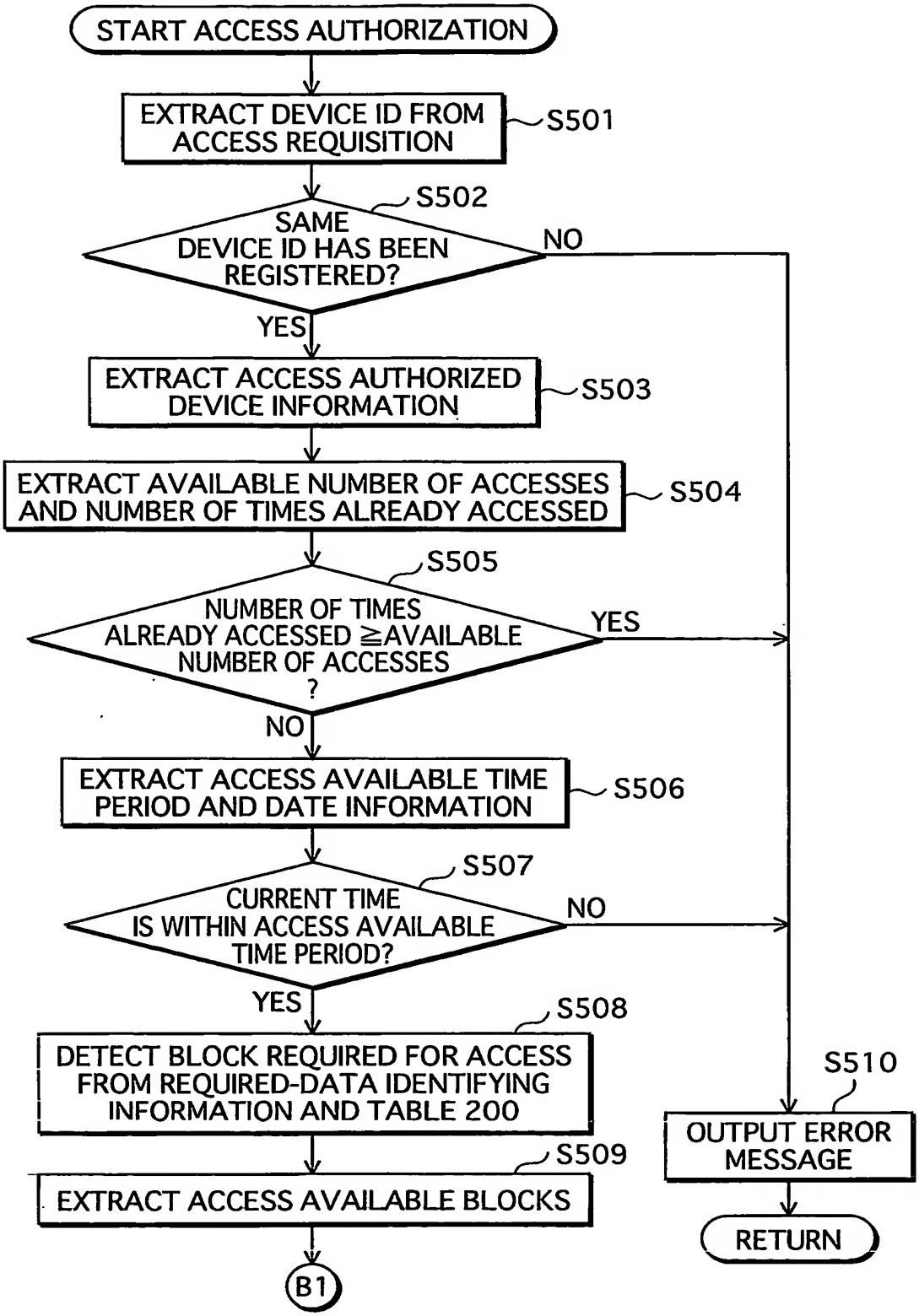
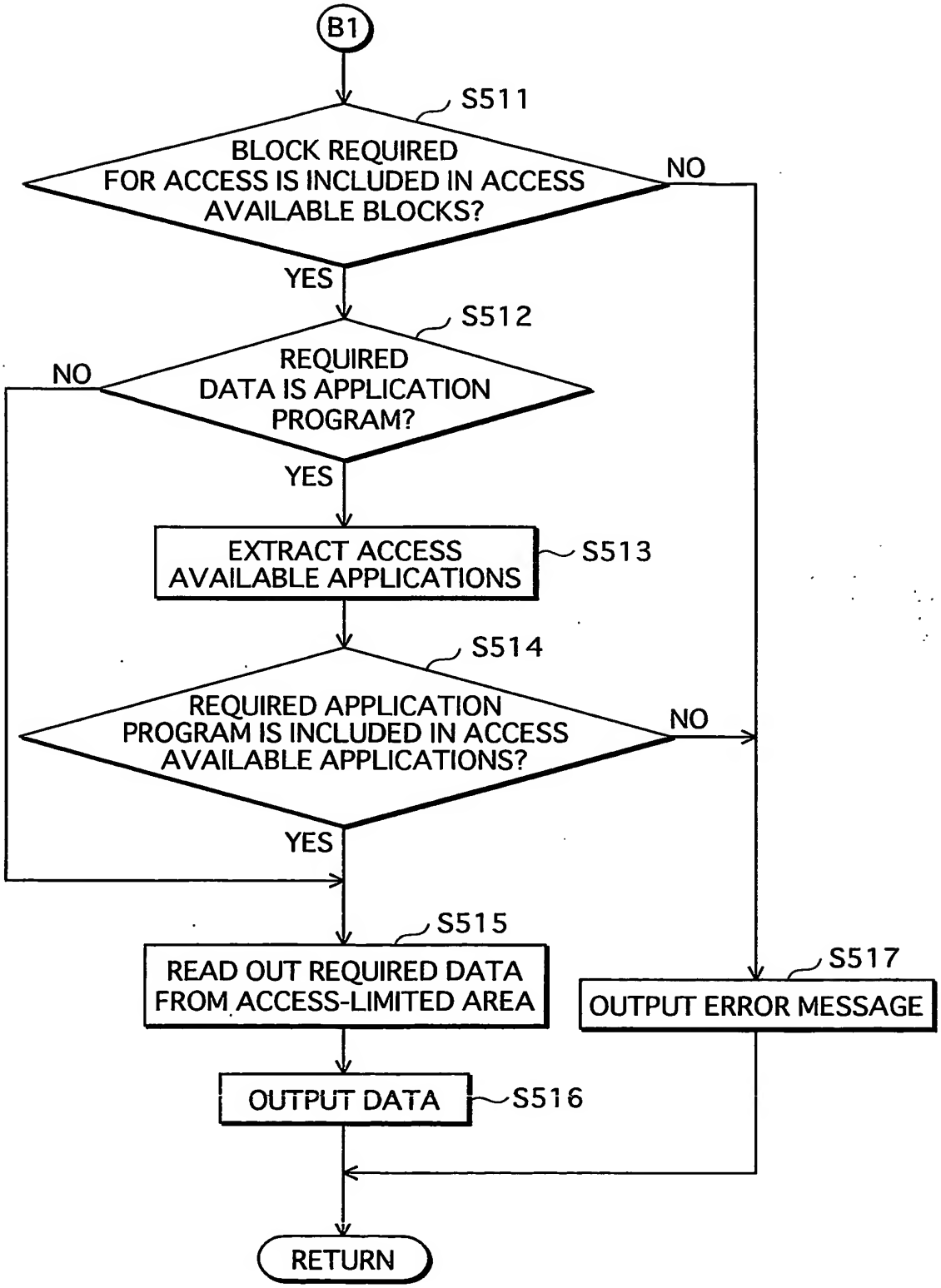

START ACCESS AUTHORIZATION
EXTRACT DEVICE ID FROM ACCESS REQUISITION
S501
S502
SAME DEVICE ID HAS BEEN REGISTERED?
NO
YES
EXTRACT ACCESS AUTHORIZED DEVICE INFORMATION
S503
EXTRACT AVAILABLE NUMBER OF ACCESSES AND NUMBER OF TIMES ALREADY ACCESSED
S504
S505
NUMBER OF TIMES ALREADY ACCESSED ≧AVAILABLE NUMBER OF ACCESSES ?
YES
NO
EXTRACT ACCESS AVAILABLE TIME PERIOD AND DATE INFORMATION
S506
S507
CURRENT TIME IS WITHIN ACCESS AVAILABLE TIME PERIOD?
NO
YES
S508
DETECT BLOCK REQUIRED FOR ACCESS FROM REQUIRED-DATA IDENTIFYING INFORMATION AND TABLE 200
S509
EXTRACT ACCESS AVAILABLE BLOCKS
B1
S510
OUTPUT ERROR MESSAGE
RETURN

FIG.23


B1
S511
BLOCK REQUIRED FOR ACCESS IS INCLUDED IN ACCESS AVAILABLE BLOCKS?
NO
YES
S512
REQUIRED DATA IS APPLICATION PROGRAM?
NO
YES
EXTRACT ACCESS AVAILABLE APPLICATIONS
S513
S514
REQUIRED APPLICATION PROGRAM IS INCLUDED IN ACCESS AVAILABLE APPLICATIONS?
NO
YES
S515
READ OUT REQUIRED DATA FROM ACCESS-LIMITED AREA
S517
OUTPUT ERROR MESSAGE
OUTPUT DATA
S516
RETURN

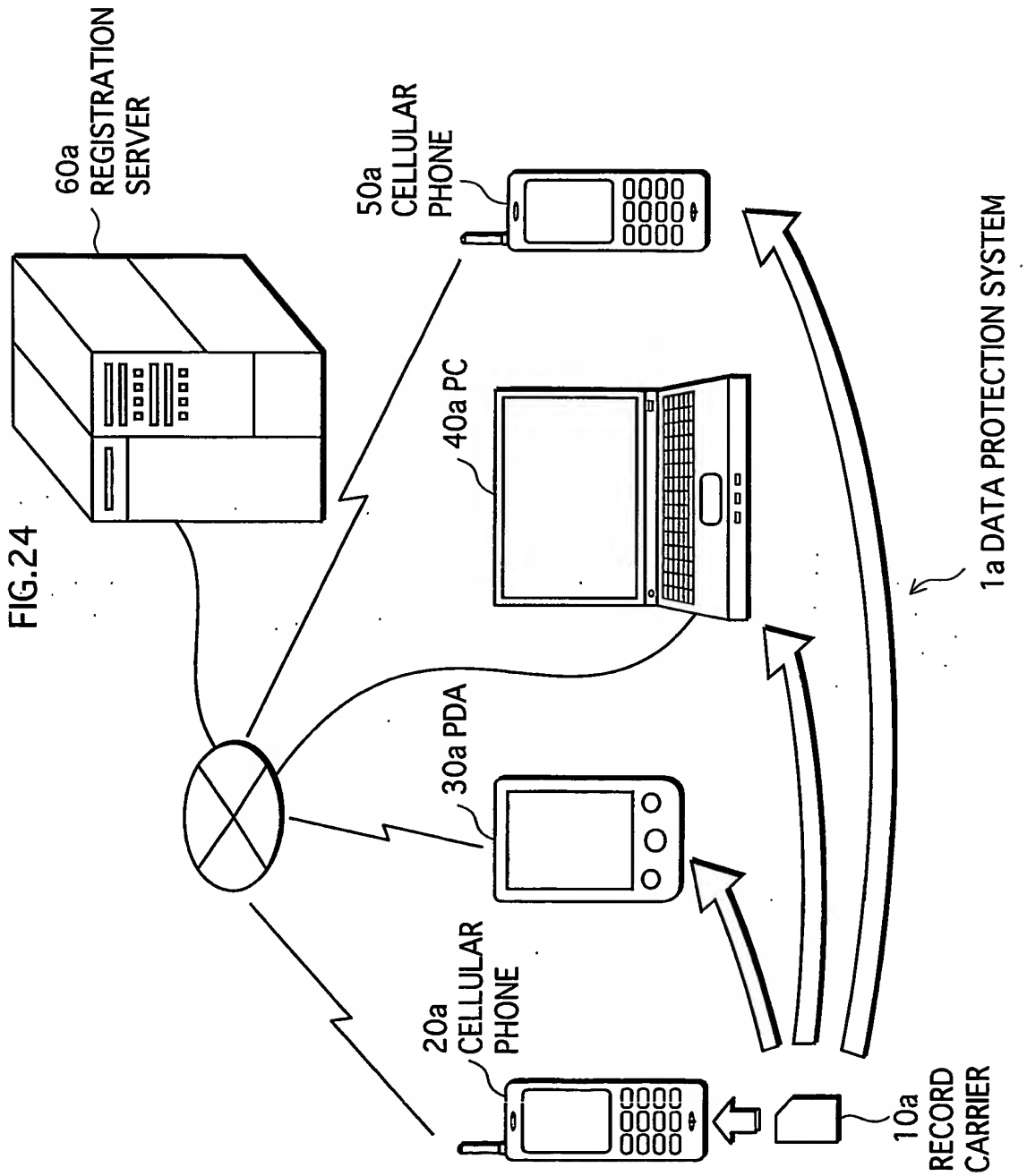

60a
REGISTRATION
SERVER
50a
CELLULAR
PHONE
40a PC
30a PDA
20a
CELLULAR
PHONE
10a
RECORD
CARRIER
1a DATA PROTECTION SYSTEM

FIG.24

FIG.25

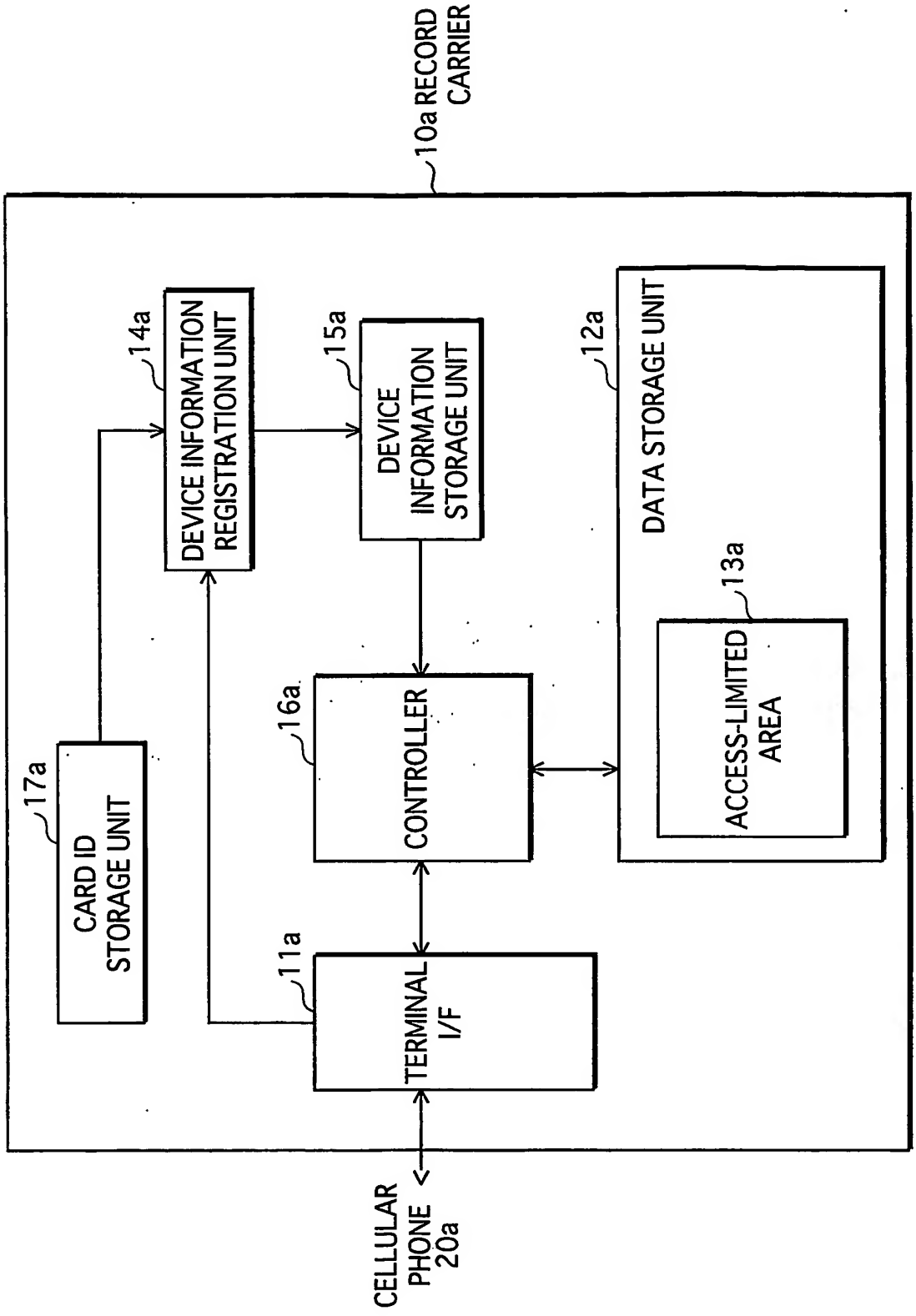

10a RECORD CARRIER
14a
DEVICE INFORMATION REGISTRATION UNIT
15a
DEVICE INFORMATION STORAGE UNIT
12a
DATA STORAGE UNIT
13a
ACCESS-LIMITED AREA
16a
CONTROLLER
17a
CARD ID STORAGE UNIT
11a
TERMINAL I/F
CELLULAR PHONE 20a

FIG.26

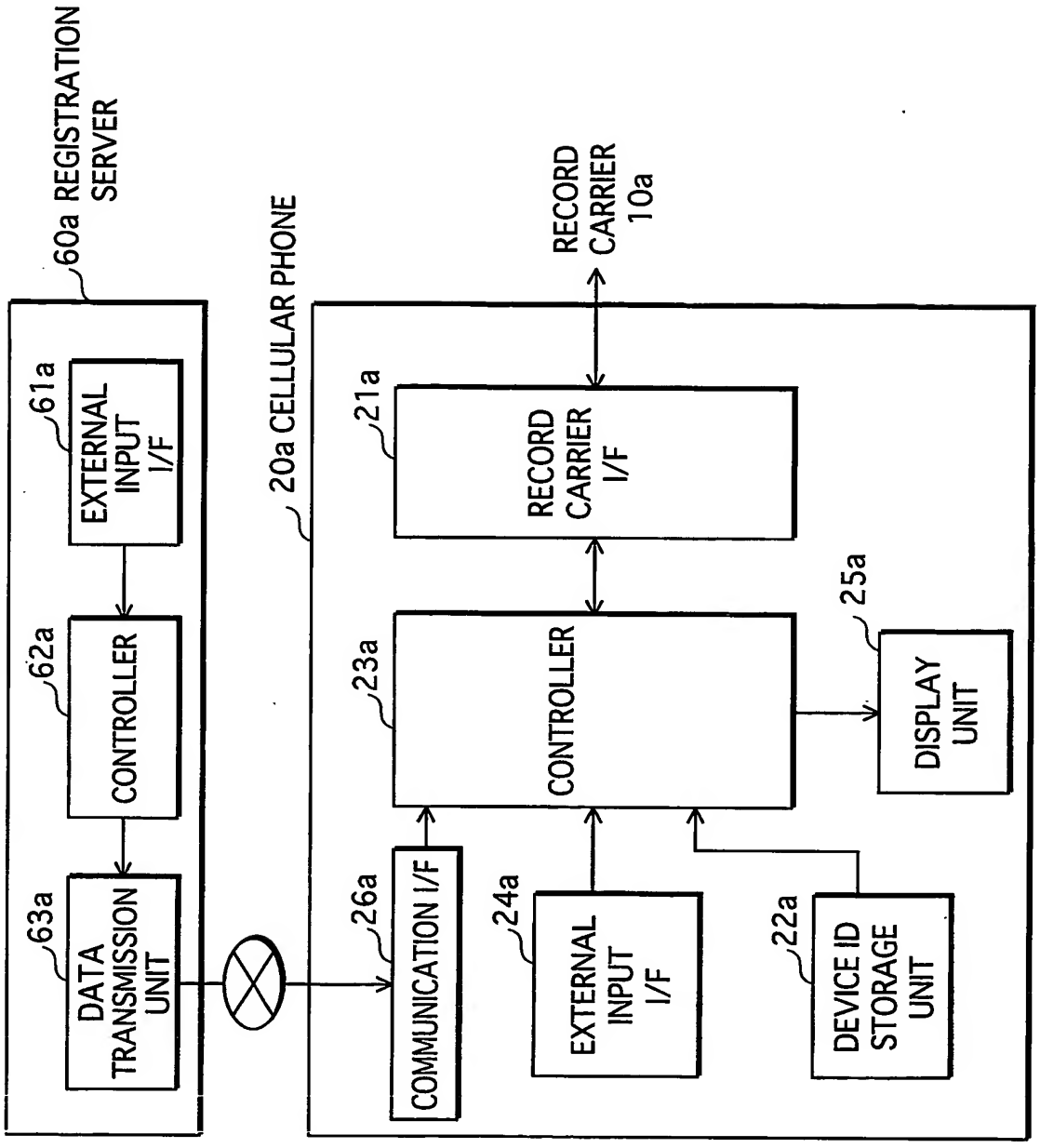

60a REGISTRATION SERVER
61a
EXTERNAL INPUT I/F
62a
CONTROLLER
63a
DATA TRANSMISSION UNIT
20a CELLULAR PHONE
RECORD CARRIER 10a
21a
RECORD CARRIER I/F
23a
CONTROLLER
25a
DISPLAY UNIT
26a
COMMUNICATION I/F
24a
EXTERNAL INPUT I/F
22a
DEVICE ID STORAGE UNIT

FIG.27

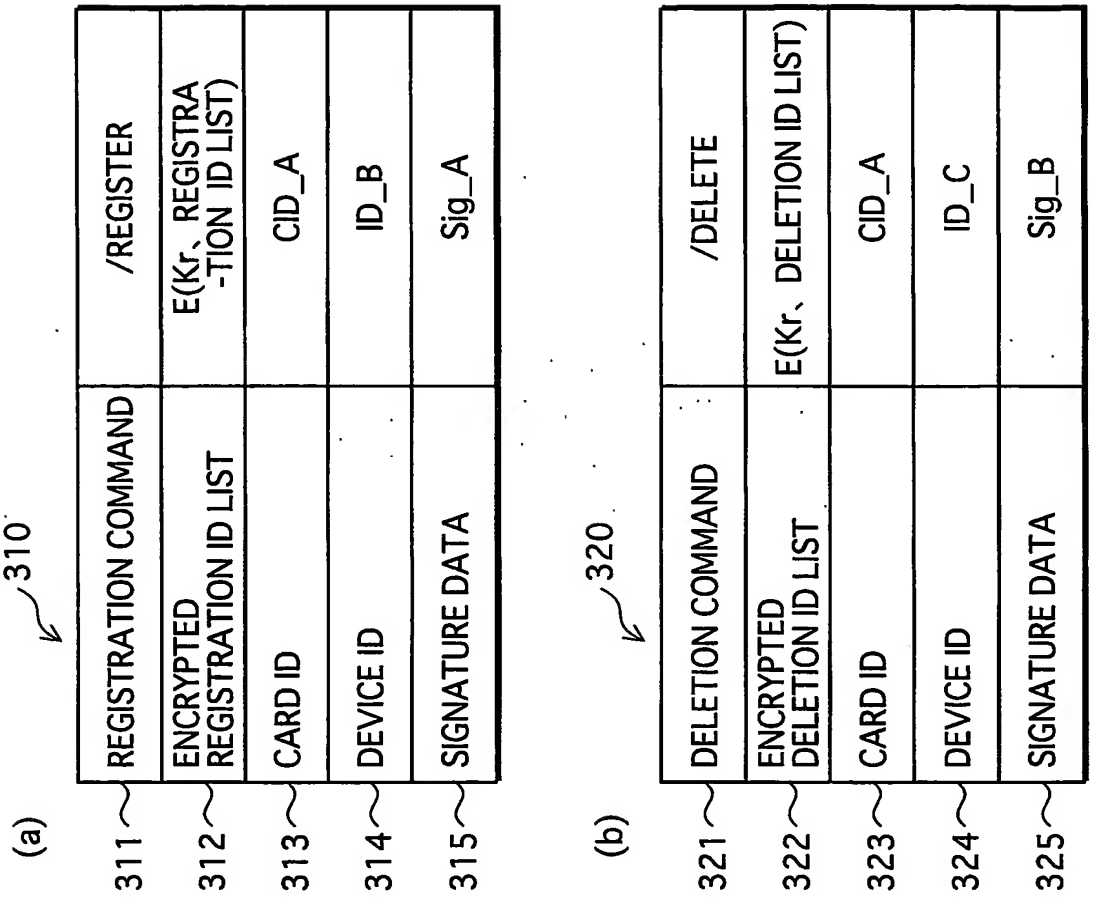

(a)
310
311
REGISTRATION COMMAND
/REGISTER
312
ENCRYPTED REGISTRATION ID LIST
E(Kr、REGISTRA -TION ID LIST)
313
CARD ID
CID_A
314
DEVICE ID
ID_B
315
SIGNATURE DATA
Sig_A
(b)
320
321
DELETION COMMAND
/DELETE
322
ENCRYPTED DELETION ID LIST
E(Kr、DELETION ID LIST)
323
CARD ID
CID_A
324
DEVICE ID
ID_C
325
SIGNATURE DATA
Sig_B

FIG.28

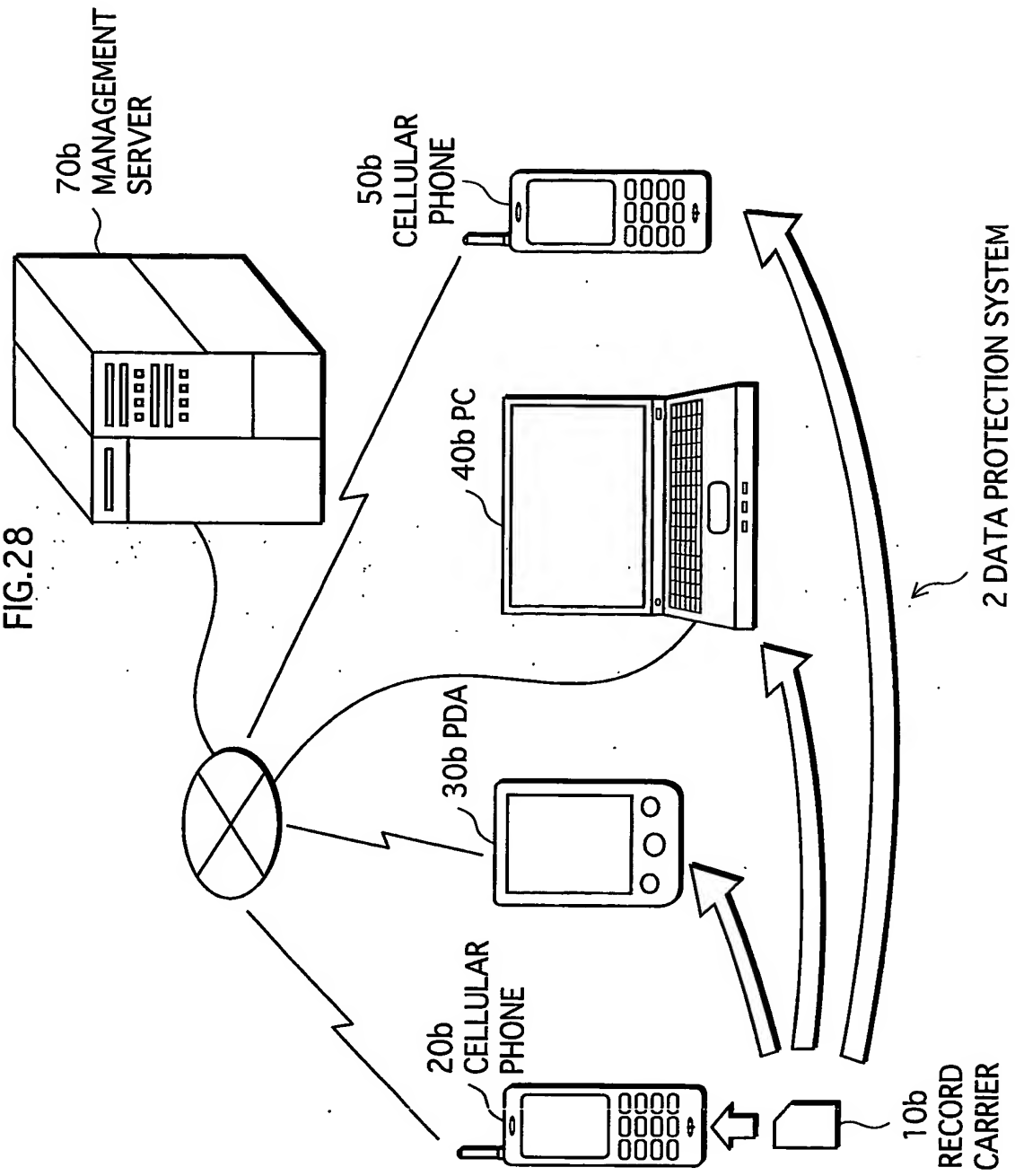

70b
MANAGEMENT
SERVER
50b
CELLULAR
PHONE
40b PC
30b PDA
20b
CELLULAR
PHONE
10b
RECORD
CARRIER
2 DATA PROTECTION SYSTEM

FIG.29

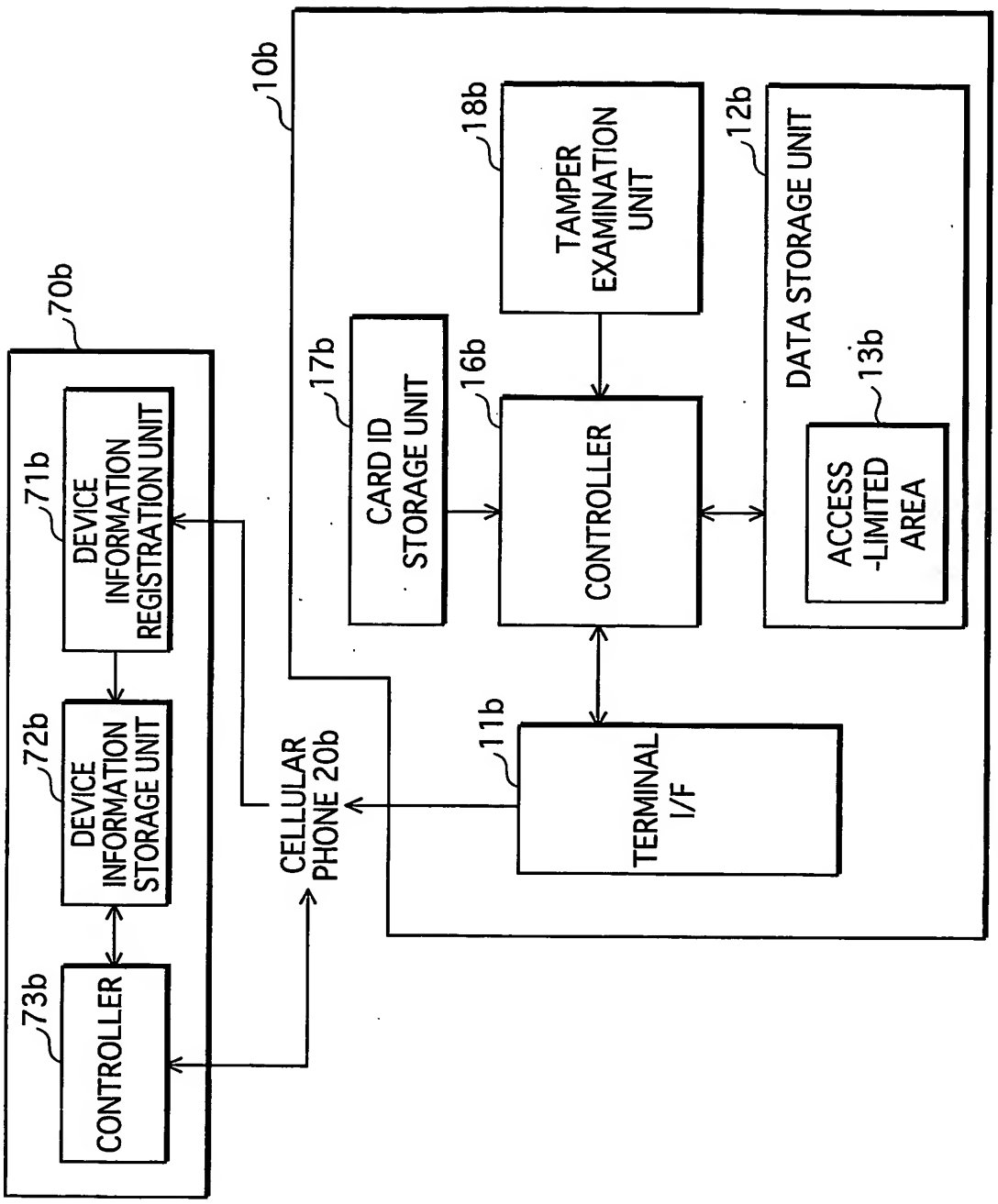

10b
18b
TAMPER EXAMINATION UNIT
12b
DATA STORAGE UNIT
13b
ACCESS -LIMITED AREA
17b
CARD ID STORAGE UNIT
16b
CONTROLLER
70b
71b
DEVICE INFORMATION REGISTRATION UNIT
72b
DEVICE INFORMATION STORAGE UNIT
73b
CONTROLLER
CELLULAR PHONE 20b
11b
TERMINAL I/F

FIG.30

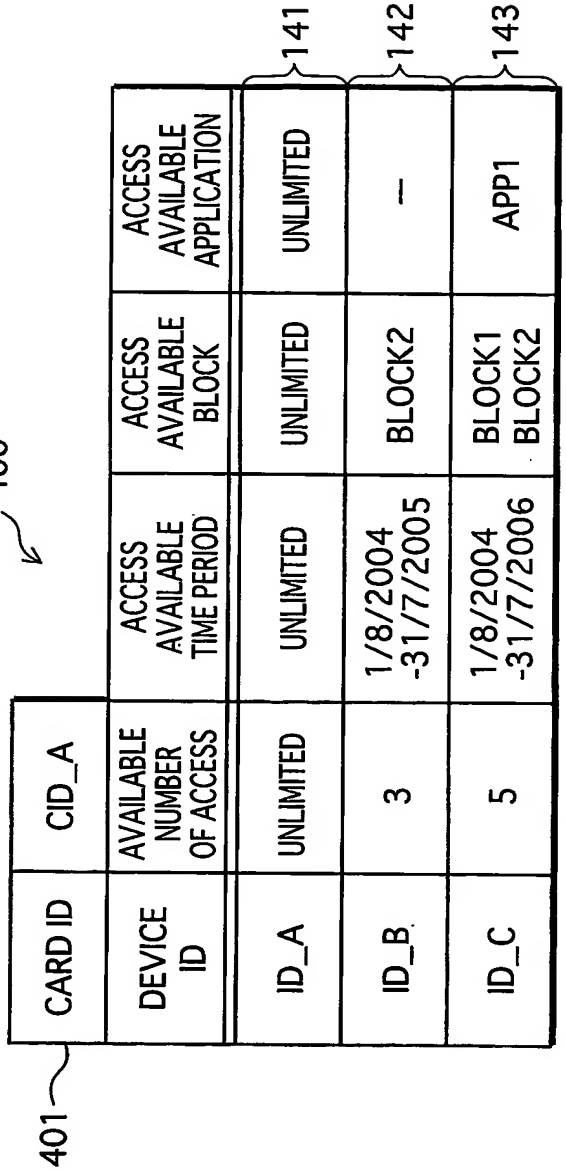

400
401
CARD ID
CID_A
DEVICE ID
AVAILABLE NUMBER OF ACCESS
ACCESS AVAILABLE TIME PERIOD
ACCESS AVAILABLE BLOCK
ACCESS AVAILABLE APPLICATION
ID_A
UNLIMITED
UNLIMITED
UNLIMITED
UNLIMITED
141
ID_B
3
1/8/2004 -31/7/2005
BLOCK2
—
142
ID_C
5
1/8/2004 -31/7/2006
BLOCK1 BLOCK2
APP1
143

FIG.31

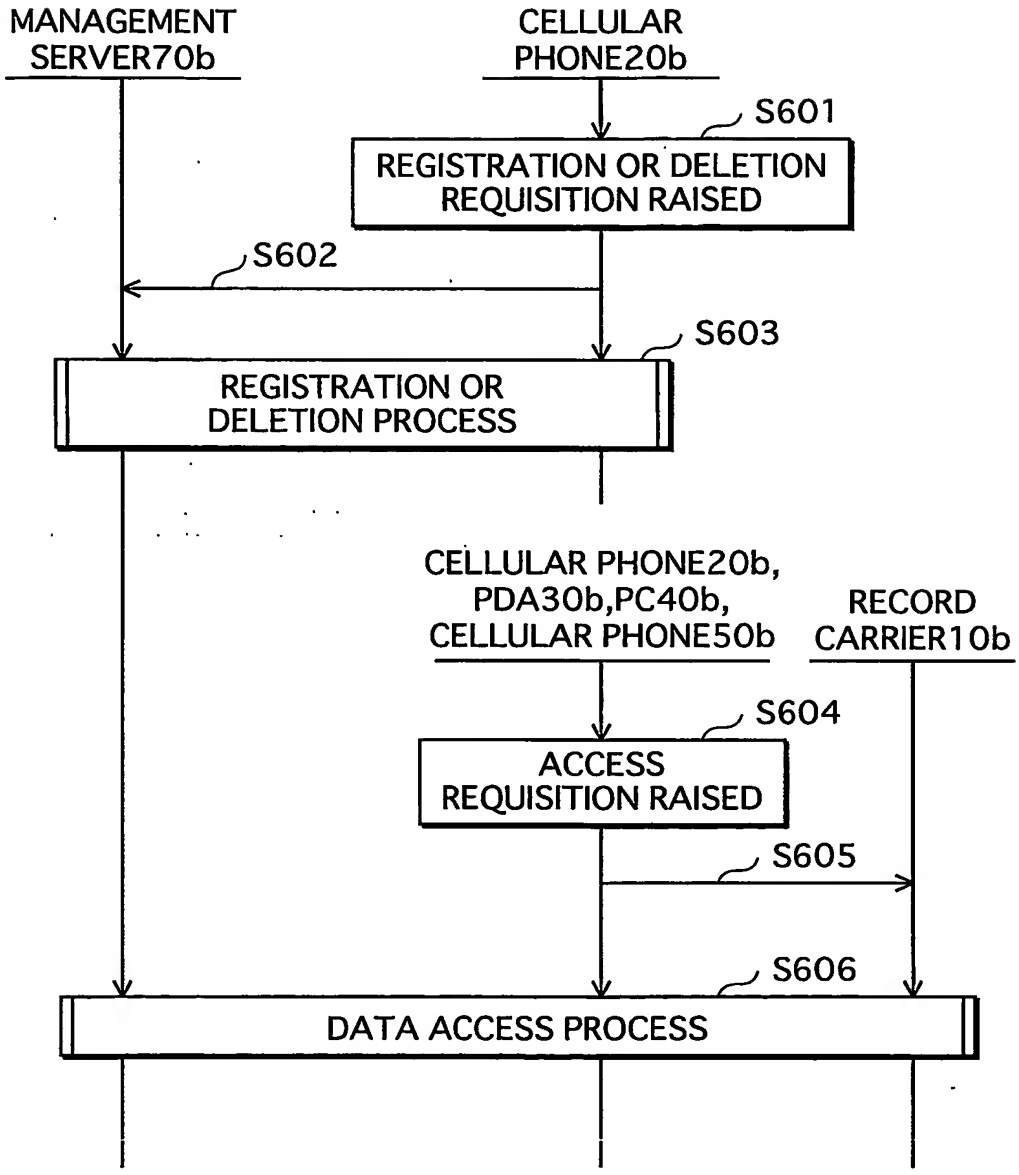
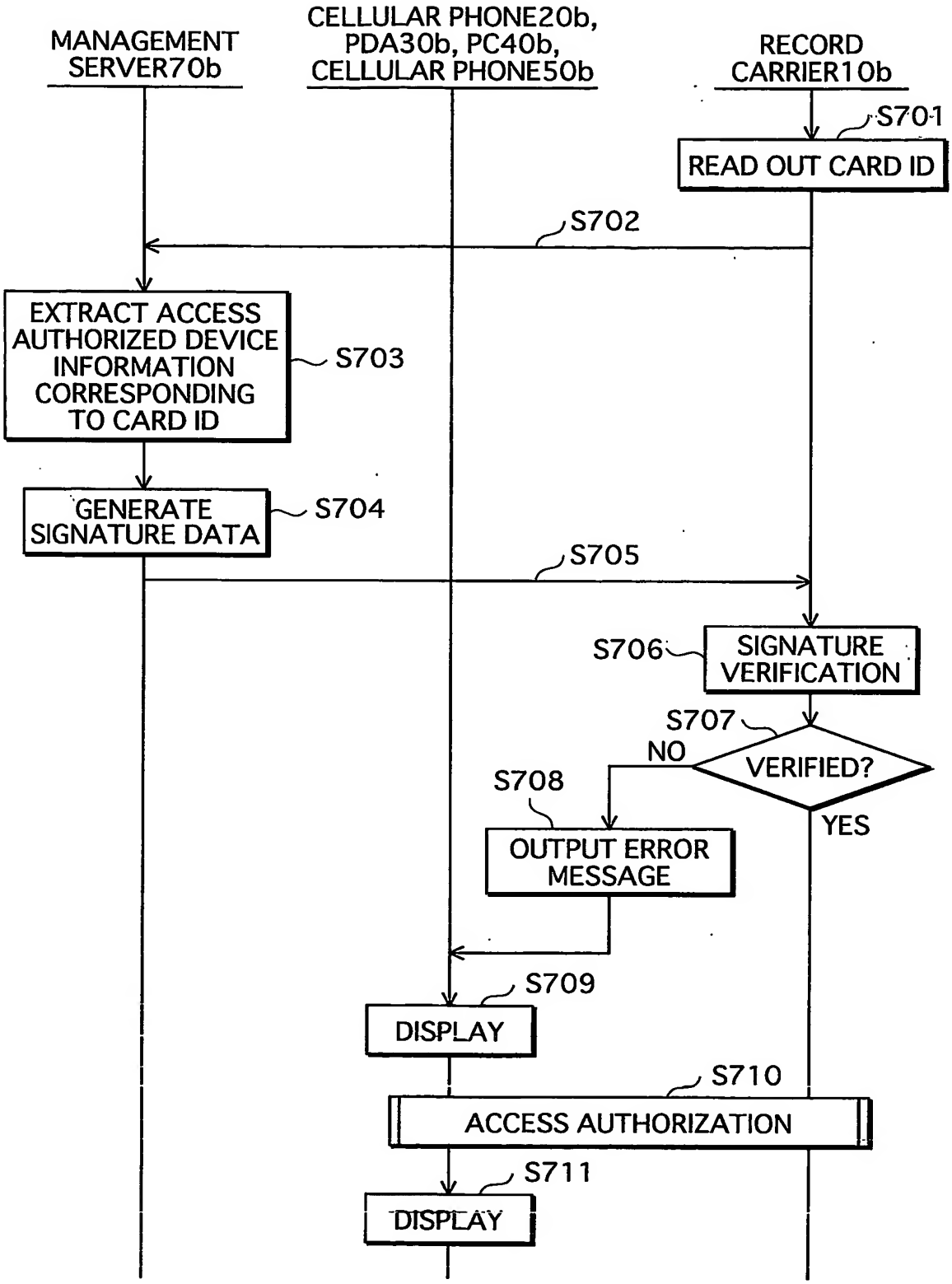

MANAGEMENT SERVER70b
CELLULAR PHONE20b
S601
REGISTRATION OR DELETION REQUISITION RAISED
S602
S603
REGISTRATION OR DELETION PROCESS
CELLULAR PHONE20b, PDA30b,PC40b, CELLULAR PHONE50b
RECORD CARRIER10b
S604
ACCESS REQUISITION RAISED
S605
S606
DATA ACCESS PROCESS

FIG.32


MANAGEMENT SERVER70b
CELLULAR PHONE20b, PDA30b, PC40b, CELLULAR PHONE50b
RECORD CARRIER10b
S701
READ OUT CARD ID
S702
EXTRACT ACCESS AUTHORIZED DEVICE INFORMATION CORRESPONDING TO CARD ID
S703
GENERATE SIGNATURE DATA
S704
S705
S706
SIGNATURE VERIFICATION
S707
VERIFIED?
NO
YES
S708
OUTPUT ERROR MESSAGE
S709
DISPLAY
S710
ACCESS AUTHORIZATION
S711
DISPLAY